GSMA

PSCEurope
Public Safety Communication Europe

CRITICAL COMMUNICATIONS IoT:

Technical Analysis of Service Levels

CONTENTS

1 Introduction

The document will present an overview of IoT from a critical communications perspective, encompassing public safety as well as business critical use, including a definition of the three main phases of emergency management. The document also covers the 4G and 5G network attributes and parameters required to facilitate efficient critical communications IoT via a number of sample use cases.

The use cases are presented in terms of their emergency management phase and include a brief summary of each scenario. In addition, the actors, data types and network attributes associated with each scenario are also detailed in order to provide the reader with a comprehensive understanding of the use of IoT technology in the area of critical communications.

This is a technical document, intended to be used by network operators and network and device equipment vendors. The document may also be useful for the public safety community to understand how IoT can be employed for their own purposes.

2 Critical Communications and Internet of Things

Communications needed to achieve a specific mission, for public safety purposes and business-critical functions, are critical and need a higher priority over other communications in the networks. These critical communications also require some means of enforcing this priority. From a confidentiality, integrity and availability perspective, the requirements exceed those of other communications. This type of communication is known as Mission Critical Communications.

Generically, the Internet of Things (IoT) describes the coordination of a network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment, i.e. sensors and actuators. These connected objects include everyday appliances and machines from many vertical industries such as vehicles, utility meters, tracking devices, vending machines, monitors and sensors, consumer electronics and wearable technology, as well as smart phones and tablets.

From a Critical Communications perspective, the term Critical Communications IoT, applies to connected objects that fulfil a public safety, emergency services or business critical function.

For scenarios where multiple communication methods are used, for example in an incident response, the use of Mission Critical Push-To-Talk (MCPTT) is specifically excluded from the analysis as this is not considered part of the IoT. The use of Mission Critical Video is included in the analysis as part of the IoT where e.g. video data is transmitted from remote CCTV cameras or body-worn cameras.

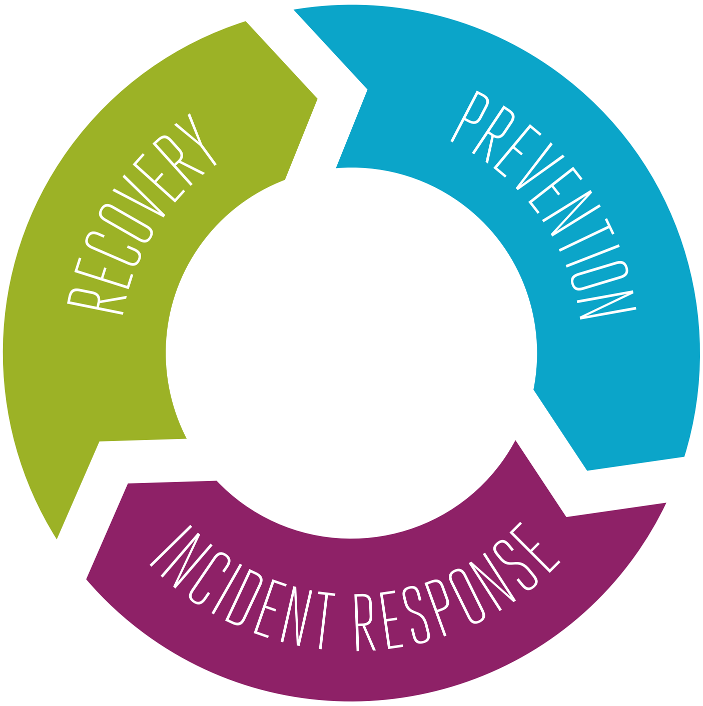
A more holistic introduction of the implementation of Mission Critcal services on 3GPP networks can be found here [1].

For the emergency services related use cases, the three main phases of emergency management are covered as defined in [2]. For each phase, the communications requirements are different, as the urgency and criticality of the information varies.The three phases are:

- **INCIDENT RESPONSE PHASE:**
  - ↘ actions taken in order to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilizing events or disruptions, and to recover to a normal situation
  - ↘ the most stringent communication requirements of the three phases, with the highest priority and lowest latency.

- **PREVENTION PHASE:**
  - measures that enable an organization to avoid, preclude or limit the impact of an undesirable event or potential disruption
  - the second most stringent communications requirements of the three phases, as the data must be received within a certain timeframe for it to be useful and meaningful in order to achieve the objectives described in the previous bullet

- **RECOVERY PHASE:**
  - restoration and improvement, where appropriate, of operations, facilities, livelihoods or living conditions of affected organizations, including efforts to reduce risk factors
  - the most relaxed communications requirements of the three phases, as there is no immediate risk if the data transmission is delayed



3 4G and 5G QoS

One of the key requirements from a mission critical perspective is the network performance. Network performance is necessary to ensure that users of the system would be able to communicate and exchange information, be it sensor data or high definition video stream, when the need arises in order to achieve their business critical function or their public safety duties.

In order to support different types of quality of service (QoS) in a packet-switched network, a mechanism is required to distinguish the different traffic types so that the traffic can be managed appropriately in the network. For example, a voice service needs stricter latency performance compared with a file transfer service, and therefore traffic related to voice services need to be processed by the network so that the latency requirement is met.

From a 4G perspective, QoS is supported via QoS Channel Indicators (QCI) which represent the type of service level provided by the 4G network. QCIs include parameters such as priority, packet delay budget and packet error loss rate. A number of standardized QCIs are defined in the 3GPP specifications [3] which is based on the requirements of a number of different services, such as conversational voice and video. For 4G, a QCI value is assigned to each EPS bearer, which means that QoS is enforced at the EPS bearer level.

From a 5G perspective, the 4G QCI definitions have been enhanced by including additional parameters: default maximum data burst volume and default averaging window. The 5G QoS indication is termed 5QI [4], based on the 4G QCI standardized values, with the introduction of a new delay-critical GBR. For 5G, 5QI is applied at the QoS flow level, which may include a number of service data flows sharing the same 5QI characteristics.

In a 5G network, 5QI forms part of a wider set of network attributes that characterizes various aspects of the network under the umbrella of network slicing [5][6]. While 5G pulls together this broader range of network attributes to help network operators offer a more targeted service to different market segments and verticals, most of these attributes already exist in 4G systems deployed today, e.g. capability to support group communications, routing user data to the internet / private networks.

4 5G Network Attributes

Network slicing is the key feature of the 5G networks and enables dedicated logical networks to be built on a shared infrastructure. These dedicated networks would allow the implementation of tailor-made functionality and network operation specific to the needs of each network slice customer, rather than a one-size-fits-all approach of previous generations of mobile networks.

In order to define the characteristics of a 5G network slice for public safety use cases in this document, a set of standardised attributes defined in the GSMA Generic Slicing Template document [8] were used. A subset of the attributes which are relevant to the critical communications IoT use cases analysed in this document are described below:

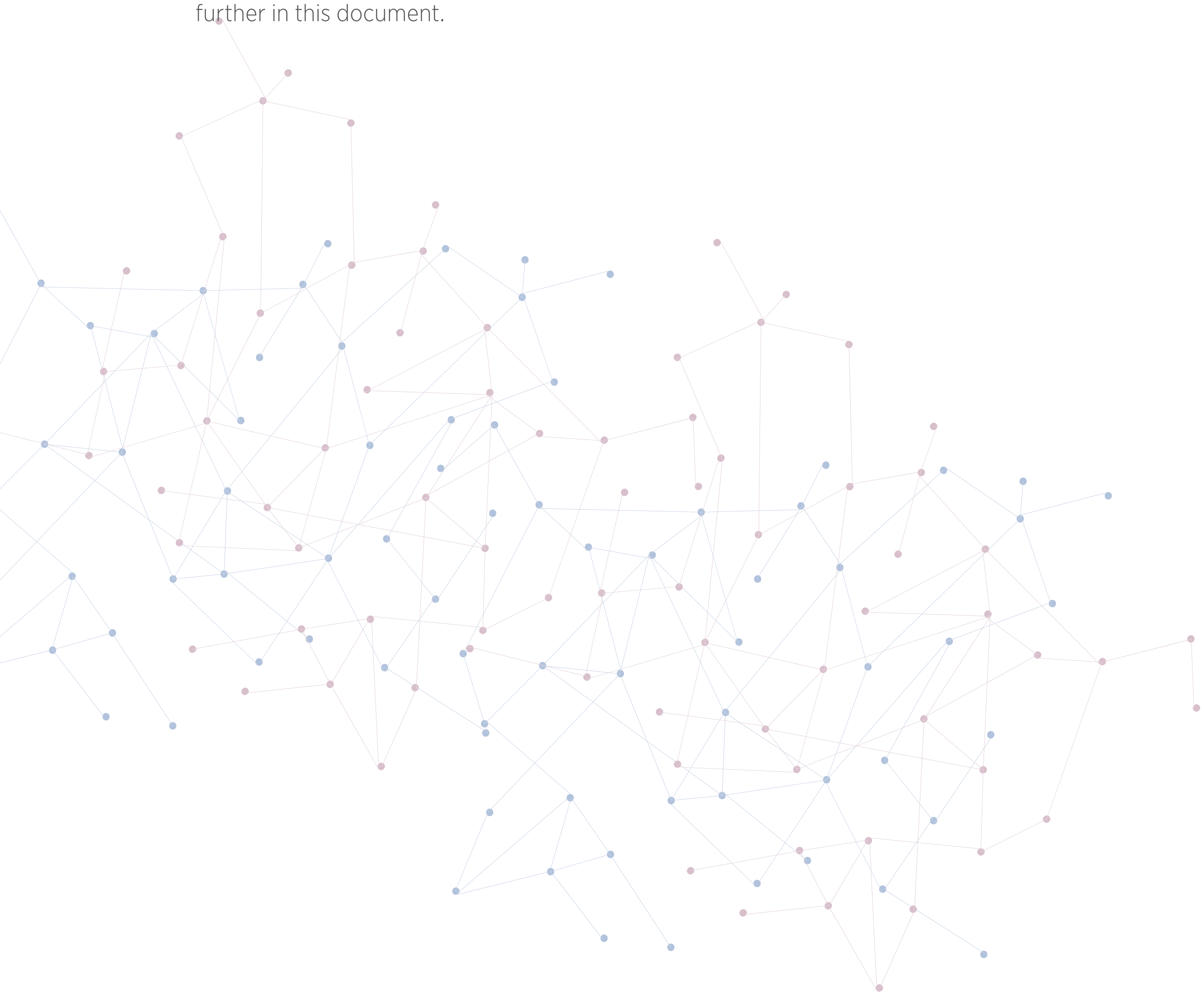
- **Deterministic communication:** user traffic with periodic transmissions
- **Downlink and Uplink Throughput per UE**
- **Group Communication Support**
  - ↘ no group communications
  - ↘ Broadcast/Multicast (MBMS): enables point-to-multipoint transmissions over a single or multiple cells
  - ↘ Single Cell Point to Multipoint (SC-PTM)[1]: supports broadcast/multicast services over single cell, and the broadcast/multicast area can be dynamically adjusted cell by cell according to user's distribution
  - ↘ Group Communications System Enablers (GCSE): service enablers in the 3GPP system making use of e.g. MBMS functionality to provide a fast and efficient mechanism to distribute the same content to multiple users in a controlled manner for applications such as MCPTT [7]. Note that GCSE is still to be defined in NG.116 [8]
- **Isolation Level:** levels of physical or logical separation between slices, depending on requirements from the network slice customer or vertical. A network slice instance may be fully or partly, logically and/or physically, isolated from another network slice instance. This attribute describes different types of isolation:
  - ↘ **Physical isolation** – network slices are physically separated (e.g. different rack, different hardware, different location)
    - ↘ Process and threads isolation
    - ↘ Physical memory isolation
    - ↘ Physical network isolation
  - ↘ **Logical** – network slices are logically separated.
    - ↘ Virtual resources isolation – a network slice has access to specific range of resources that do not overlap with other network slices e.g. Virtual Machine (VM) isolation

[1] https://www.3gpp.org/technologies/keywords-acronyms/1763-sc_ptm

        - Network functions isolation – Network Function (NF) is dedicated to the Network Slice Customer (NSC), but virtual resources are shared
        - Tenant/Service Isolation – Network Slice Customer (NSC) data are isolated from other NSCs, but virtual resources and Network Functions (NFs) are shared

- **Location based message delivery:** used to distribute information, e.g. signalling messages, to terminals within a specific geographical area
- **Mission Critical support:** leads to a priority of the network slice relative to others, for Control Plane and User Plane decisions
    - **Mission-critical capability support:** specifies what capabilities are available to support mission-critical services. More than one capability may be supported at once
        - Inter-user prioritization – provides admission and the scheduling of priorities for PS (Packet Service) users over non-PS users, and different priorities among PS users
        - Pre-emption – allows non-PS users to be pre-empted by PS users, and a PS user to be pre-empted by another PS user
        - Local control – allows dynamic and temporary assignment of inter-user prioritization and pre-emption levels to local PS users (e.g. local to an incident)
    - **Mission-critical service support:** specifies whether or not the network slice supports:
        - mission-critical push-to-talk (MCPTT) [12]
        - mission-critical data (MCData) [13]
        - mission-critical video (MCVideo) [14]
        - Isolated E-UTRAN Operation for Public Safety (IOPS) [15], [16], describing a typical scenario where a portable base station is used to temporarily provide local network coverage for public safety personnel at an incident site where there is no / poor network coverage. Note that this document includes use cases under network coverage only, so excludes use cases requiring IOPS.
        - mission-critical interworking with TETRA / P25 systems [17].
        - mission-critical system migration and interconnection which enables 1) public safety users to utilise a mission critical system outside their home network e.g. in a roaming scenario, and also 2) public safety users in one mission critical system to communicate with public safety users on a different mission critical system. Note that this option is still to be defined in NG.116 [8]
- **MMTel Support:** whether IMS and MMTel support is needed
- **Slice QoS parameters:** as defined in 3GPP TS 23.501 [4], Table 5.7.4-1, which maps to specific priority levels, packet delay budgets, packet error rates and other parameters. The 5G QoS characteristics with pre-configured 5QI values from this table are pre-configured in the Access Network. The 5G QoS characteristics for QoS Flows with dynamically assigned 5QI are signalled as part of the QoS profile. Note that the standardized 4G QCI values defined in 3GPP TS 23.203 [3] form the basis of the 5QI values, and therefore, the standardized 5QI values defined in this document may be used for the 4G QCI.

- **User data access:** routing of data – locally only, private network, open internet
  - The device has access to the Internet
  - All data traffic is routed to the private network e.g. via tunnelling mechanism such as L2TP and VPN (Virtual Private Network)
  - All data traffic stays local and the devices do not have access to the Internet or private network
- **Number of terminals:** maximum number of terminals supported by the network slice. Note: This is a scalability attribute and the value depends on the actual deployment scenario and from region to region, so will not be covered further in this document.
- **Terminal Density:** maximum number of connected and/or accessible devices supported per unit area (per km^2). Note: This is a scalability attribute and the value depends on the actual deployment scenario and can vary from incident to incident, so will not be covered further in this document. In the case of a very large incident or event, there can be a very large number of first responders and terminals. For example, for the London 2012 Olympics, 40,000 security personnel were deployed[2], excluding medical and fire personnel.



[2] https://en.wikipedia.org/wiki/Security_for_the_2012_Summer_Olympics

The parameters are represented in the following table.

ATTRIBUTE NAME	VALUE	UNIT	COMMENTS
Deterministic communication		n/a	user traffic with periodic transmissions 0: not supported 1: supported
Downlink throughput per UE		Kbps	
Uplink throughput per UE		Kbps	
Group Communication Support		n/a	0: not available 1: Single Cell Point to Multipoint (SC-PTM) 2: Broadcast/Multicast 3: Broadcast/Multicast + SC-PTM 4: Group Communications System Enablers (GCSE) Note: value 4 is still to be defined in NG.116 [8]
Isolation Level		n/a	0: No Isolation 1: Physical Isolation 2: Logical Isolation
Location based message delivery		n/a	used to distribute information, e.g. signalling messages, to terminals within a specific geographical area 0: not supported 1: supported
Mission Critical support		n/a	leads to a priority of the network slice relative to others, for Control Plane and User Plane decisions
Mission-critical capability support		n/a	specifies what capabilities are available to support mission-critical services. More than one capability may be supported at once 1: Inter-user prioritization 2: Pre-emption 3: Local control
Mission-critical service support		n/a	1: MCPTT 2: MCData 3: MCVideo 4: IOPS 5: MC interworking with LMR system 6: MC system interconnection and migration Note: value 6 is still to be defined in NG.116 [8]
MMTel Support		n/a	whether IMS and MMTel support is needed 0: not supported 1: supported
Slice QoS parameters		n/a	5G QoS characteristics for pre-configured 5QI values are pre-configured in the Access Network. The 5G QoS characteristics for QoS Flows with dynamically assigned 5QI are signalled as part of the QoS profile. Standardised 5CI can be mapped to the standardised 4G QCI values for the purposes of this document.
User data access		n/a	0: Direct internet access 1: Termination in the private network 2: Local traffic (no internet access)

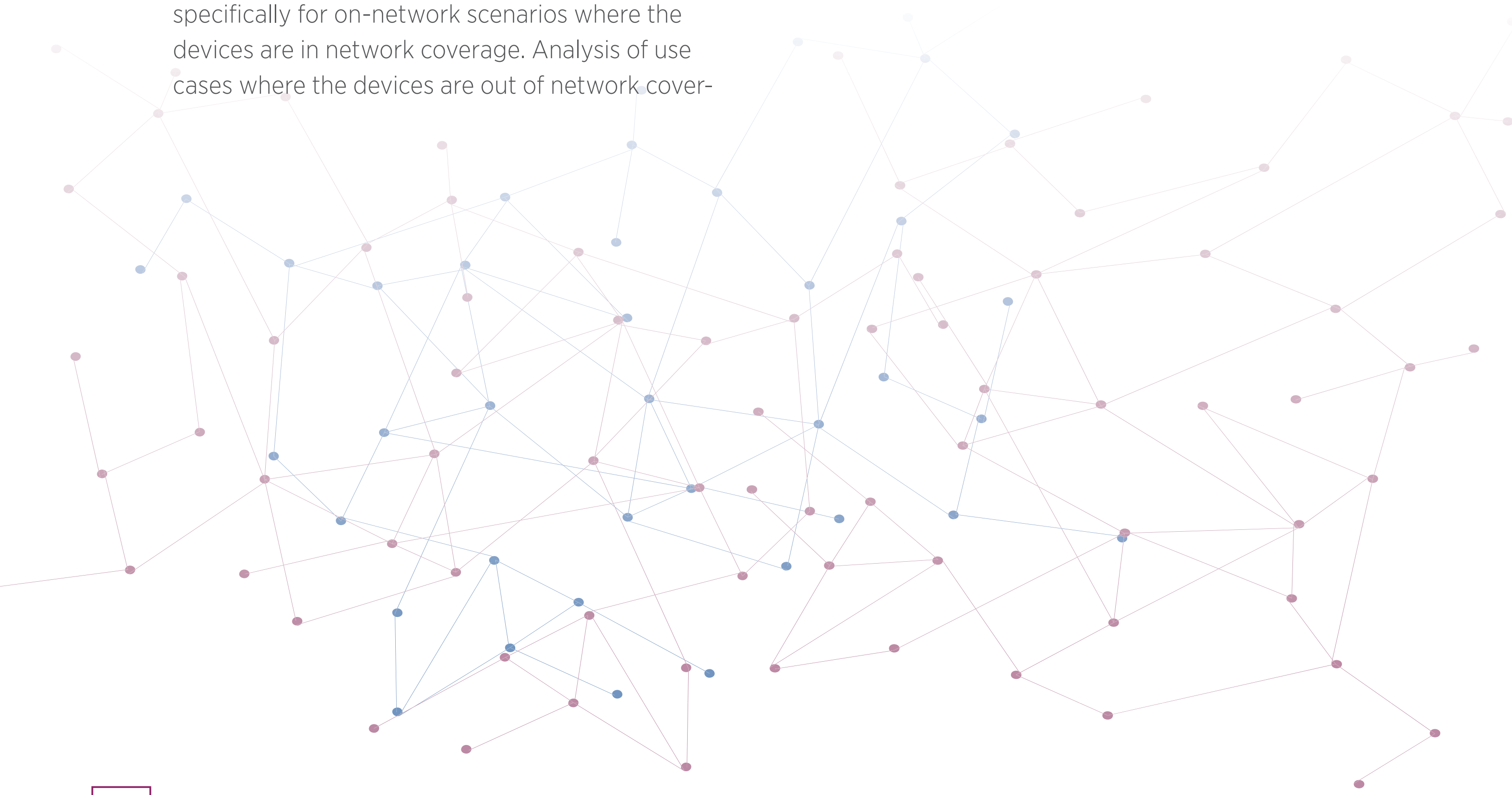
5 Critical Communications IoT Use Cases

When it comes to mission critical communications IoT use cases from a public safety perspective, there are a few documents already available that define such use cases in more detail [9][10][11]. Where relevant use cases have already been defined in the references, this document makes use of those in the analysis.

The aim of this section is to provide an overview of critical communications IoT use cases for both public safety and business critical aspects. For the public safety use cases, these are distinguished further into each of the three phases of emergency management described previously: prevention, incident response and recovery.

The public safety use cases analysed in this section are a small subset of the overall set of use cases, specifically for on-network scenarios where the devices are in network coverage. Analysis of use cases where the devices are out of network coverage are not in scope of this document. Therefore, 3GPP features such as ProSe (proximity-based services) and IOPS (Isolated E-UTRAN Operation for Public Safety) are not covered.

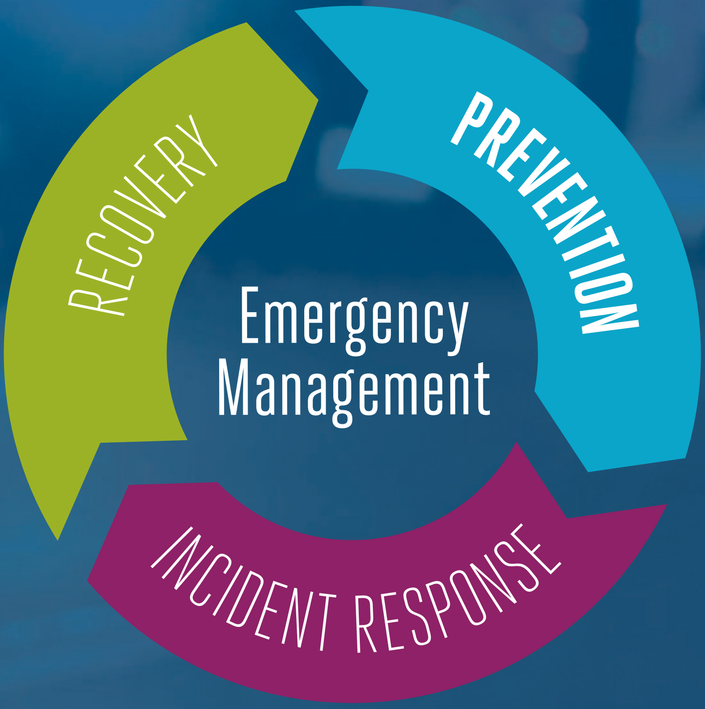
For the public safety use cases, in order to provide an understanding of the performance requirements for a network slice that would support these use cases, the performance attributes described in the previous section are derived and tabulated.



PREVENTION PHASE: FIRST RESPONDERS HEALTH AND SAFETY STATUS

While first responders are on their normal day-to-day duties, regardless of whether they are involved in an incident response, information on their health and safety status is important in order to safeguard their wellbeing. Having their health and safety status available to nearby colleagues as well as to a control room can also help determine if any event turns into a life-and-death scenario or an emergency where a quick response from the relevant teams can help save the first responders' life or resolve an escalating situation.

Various sensors can be fitted on the uniform or equipment of first responders, that can measure their health status such as heart rate, respiratory rate and body temperature. Other sensors can also be fitted in order to monitor the environment that the first responder is in, measuring things such as the environmental temperature and presence of any toxic gases or chemicals. Additionally, sensors that detect motion and state of the first responder (at rest, running, lying motionless, etc) can help indicate whether additional support is needed. Also, depending on the first responder function, different sensors can be included, such as the level of oxygen available in the tank for firefighters.



ACTORS

Example of the actors involved in this use case are:

- Firefighters
- Medical personnel
- Law enforcement personnel

DATA TYPES

The sensor data transmission is characterised as very low throughput with a periodic or event-triggered nature transmission. The sensor data types can be described as follows:

- Biometrics measuring: heart rate, perspiration, temperature, respiratory rate, oxygen saturation, sugar levels.
- Physical trackers detecting: steps taken, direction of travel, GPS coordinates of the wearer, motion and physical state of wearer (at rest, running, lying motionless, etc)
- Environmental sensors detecting: smoke, heat / temperature, carbon monoxide and carbon dioxide, noxious gases, chemicals.

Some types of sensor data, such as the GPS co-ordinates of the wearer, is typically sent at defined intervals. Other sensor data, such as the environmental and biometrics, would typically be transmitted on an event-triggered basis depending on e.g. changes from expected values. For the event-triggered transmissions, the data sent may also include historical measurement data.

Assumptions are made below on the amount of data to be transmitted and the frequency of transmissions for the different types of data described above:

BIOMETRICS	ESTIMATED MESSAGE SIZE (KB)	ESTIMATED INTERVAL BETWEEN TRANSMISSION(S)
Heart rate	0.001	10
Perspiration	0.001	300
Temperature	0.001	60
Respiratory rate	0.001	10
Oxygen saturation	0.001	10
Sugar levels	0.001	60

PHYSICAL TRACKERS	ESTIMATED MESSAGE SIZE (KB)	ESTIMATED PERIODICITY (S)
Mobility (direction of travel, number of steps taken)	0.001	60
Determined location of wearer (e.g. GPS, Galileo)	0.01	60

ENVIRONMETAL SENSING	ESTIMATED MESSAGE SIZE (KB)	ESTIMATED INTERVAL BETWEEN TRAMISSIONS (S)
Smoke detection	0.001	60
Heat detection	0.001	60
Carbon monoxide and carbon dioxide	0.001	60
Noxious gasses	0.001	60
Chemicals	0.001	60
Environmental temperature	0.001	60

Based on these assumptions, the following data throughput is required for a single actor:

Data type	**THROUGHPUT [KB/S]**	**DIRECTION**
Sensor data estimated throughput	0.0006	uplink

It is further assumed the throughput calculated above would also apply for other use cases with different types of sensors than those described above for various types of public safety agents such as firefighters, police officers, including vehicles and robots used in the field. This is because each public safety agent may not use all the sensor types listed, and may use others with similar throughput characteristics. Therfore, throughout this document, where sensor data is included in the use case, the throughput calculated here is used.

NETWORK ATTRIBUTES

The following table describes the network slicing attributes for the sensor data types described in the previous section.

Note that the throughput values indicated have been rounded based on the calculations in the previous section.

ATTRIBUTE NAME	SENSOR DATA	UNIT	COMMENTS
Deterministic communication	1	n/a	user traffic with periodic transmissions 1: supported Note: the periodicity value(s) is dependant on the actual use case and not documented here
Downlink throughput per UE	1	Kbps	Note: throughput values defined here are an average based on assumptions made for this specific use case
Uplink throughput per UE	1	Kbps	Note: throughput values defined here are an average based on assumptions made for this specific use case
Group Communication Support	0	n/a	0: not available 1: Single Cell Point to Multipoint (SC-PTM) 2: Broadcast/Multicast 3: Broadcast/Multicast + SC-PTM 4: Group communications system enablers (GCSE) Note: no group communications envisaged for this use case
Isolation Level	2	n/a	2: Logical Isolation Note: exact implementation option is subject to the local organisation and country requirements
Location based message delivery	0	n/a	used to distribute information, e.g. signalling messages, to terminals within a specific geographical area 0: not supported
Mission Critical support	1	n/a	leads to a priority of the network slice relative to others, for Control Plane and User Plane decisions 1: mission-critical
Mission-critical capability support	2	n/a	specifies what capabilities are available to support mission-critical services. More than one capability may be supported at once 1: Inter-user prioritization 2: Pre-emption 3: Local control
Mission-critical service support	2, 5	n/a	1: MCPTT 2: MCData 3: MCVideo 4: IOPS 5: MC interworking with LMR systems 6: MC system interconnection and migration Note: where LMR systems are being used in conjunction with 3GPP-based solutions, interworking with LMR systems must be enabled
MMTel Support	0	n/a	whether IMS and MMTel support is needed 0: not supported 1: supported
Slice QoS parameters	5	n/a	5G QoS Identifier (5QI)
User data access	0	n/a	0: Direct internet access Note: direct internet access via proxy with whitelisting / black-listing

INCIDENT RESPONSE: HOUSE FIRE

RECOVERY
PREVENTION
Emergency Management
INCIDENT RESPONSE

The details of this use case can be found in document in [9] section 5.2, summarised as follows:

Incident response to a single family residential house fire where firefighters enter a burning house to perform a search and rescue operation. The focus is on IoT devices and applications that support firefighter health and safety, and situational awareness.

ACTORS

The actors considered in this use case are firefighters equipped to enter a burning house, to perform search and rescue.

DATA TYPES

The types of data can be grouped as follows:

- **Sensor data:** with typically very low throughput and transmitted in a periodic or event-triggered nature, as defined in the previous prevention phase use case
- **Video data:** High throughput data of a streaming nature collected using body-worn and other video equipment including:
  - Thermal imaging
  - Video cameras
  - Lidar

- **Request / response** type of data triggered by a request or by sending feedback either from a firefighter, the incident commander or control room.
  - The firefighters can request data or send feedback via data input methods described below:
    - Touch: wearable keyboard or wearable buttons can be used for sending additional information.
    - Gesture: using smart gloves, detailed pre-defined data sets can be selected for display via different hand gestures. For example requesting team status activates a specific firefighter's camera and video is shown to the requester.
    - Proximity: Smart mask detecting specific hand gestures in its proximity can trigger certain commands. For example, swiping hand down across the mask, activates thermal imaging overlay.
    - Voice: audio response from firefighter reporting requested information
    - Images: photos sent as a response from firefighter reporting requested information
    - 'Man down' alert in case of an emergency situation
- The firefighters can receive data or feedback via the methods described below:

- Audio alerts: through headsets or speakers
- Visual alerts: via head-up mask display
- Visual feedback: on-demand data e.g. on the back of the glove via AR
- Haptic vibration alerts

Assumptions are made below on the throughput for the data types described above:

VIDEO DATA THROUGHPUT KB/S]	THROUGHPUT KB/S]
Uncompressed thermal imaging	125,000
Camera	8,000
Lidar	166,667

REQUEST / RESPONSE FROM FIREFIGHTER	THROUGHPUT [KB/S]
Gesture (smart gloves, proximity)	0.01
Voice	32
Images	12.8
‘Man down’ alert	0.0001

REQUEST / RESPONSE TO FIREFIGHTER	THROUGHPUT [KB/S]
Head-up display (augmented reality)	2,000
Haptic vibration alerts	0.0067
Audio alerts	32
Visual indicators for biometrics, environmental temperature	0.043

Based on these assumptions, the following data throughput is required for a single firefighter:

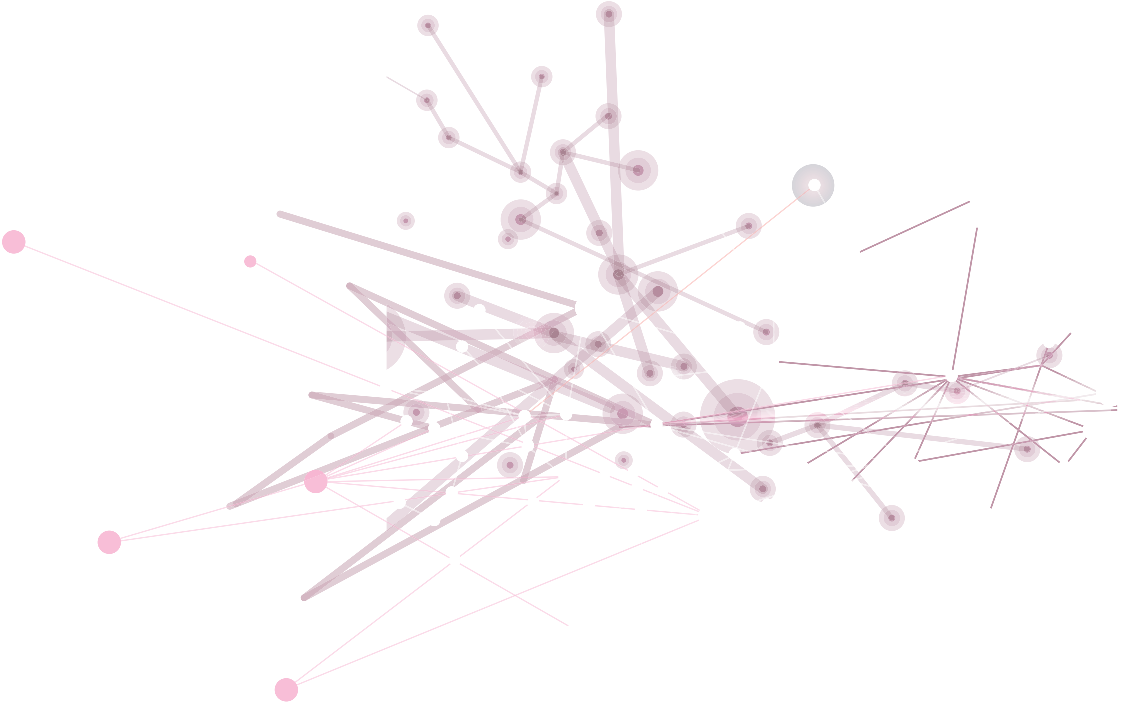
Data type	**THROUGHPUT [KB/S]**	**DIRECTION**
Total uplink throughput, consisting of:	299,711	uplink
Sensor data	0.0006	uplink
Video data	299,667	uplink
Request / response data	44.8	uplink
Total downlink throughput, consisting of:	2,032	downlink
Request / response data	2,032	downlink

NETWORK ATTRIBUTES

The following table describes the network slicing attributes for three data types described in previous sections:

- Sensor data
- Request / response
- Video data

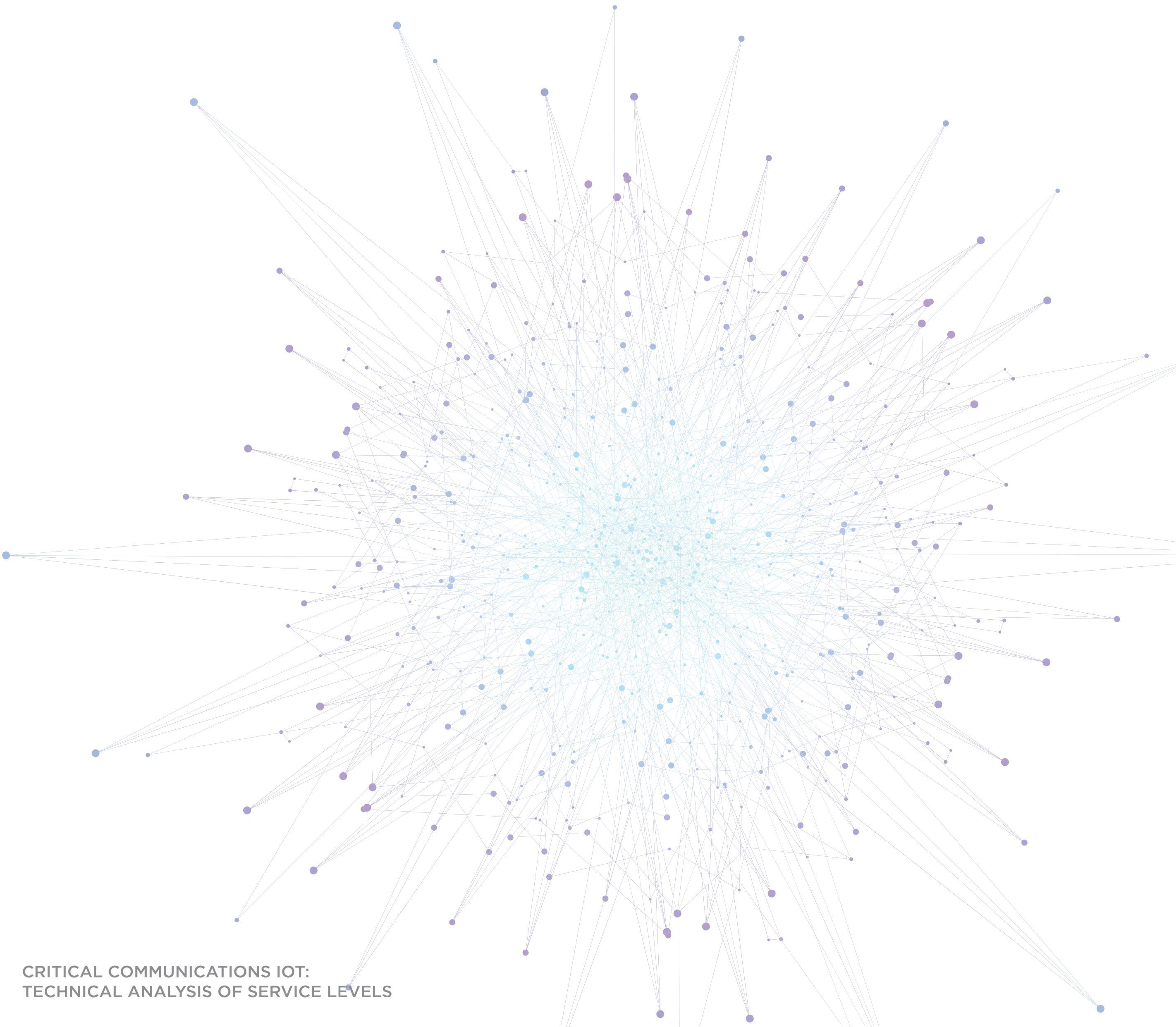
Note that the throughput values indicated have been rounded based on the calculations in the previous section.



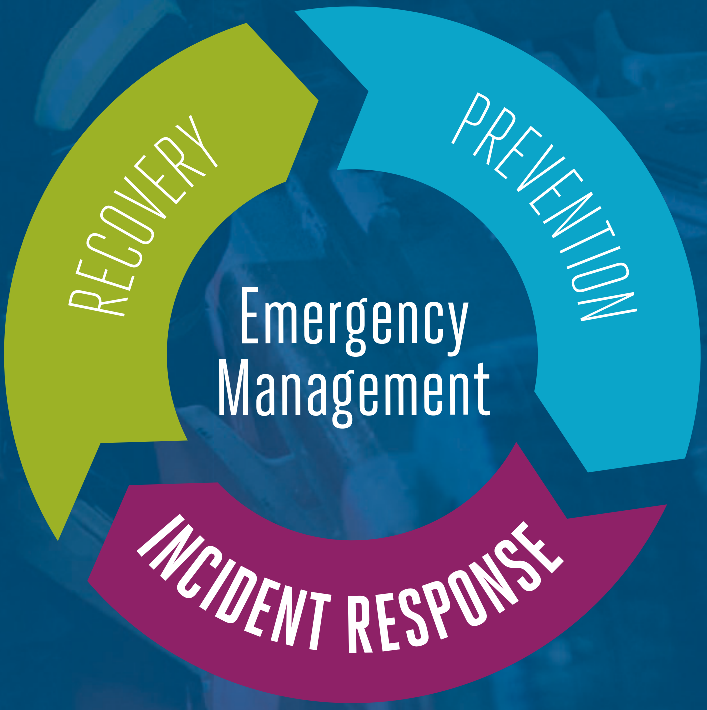
ATTRIBUTE NAME	SENSOR DATA	REQUEST / REPONSE[3]	VIDEO DATA	UNIT	COMMENTS
Deterministic communication	1	0	0	n/a	0: not supported 1: supported Note: where deterministic communications is required, the periodicity value(s) is dependant on the actual use case and not documented here
Downlink throughput per UE	1	2,000	300,000	Kbps	Note: throughput values defined here are based on assumptions made for this specific use case Video: Typically UEs will be either transmitting or receiving video at any one time. However, there will be a mix of UEs, some will be transmitting and others will be receiving.
Uplink throughput per UE	1	50	300,000	Kbps	Note: throughput values defined here are based on assumptions made for this specific use case Video: Typically UEs will be either transmitting or receiving video at any one time. However, there will be a mix of UEs, some will be transmitting and others will be receiving.
Group Communication Support	0	0	2, 3, 4	n/a	0: not available 1: Single Cell Point to Multipoint (SC-PTM) 2: Broadcast/Multicast 3: Broadcast/Multicast + SC-PTM 4: Group communications system enablers (GCSE) Note: no group communications envisaged for this use case
Isolation Level	2	2	2	n/a	0: No Isolation 1: Physical Isolation 2: Logical Isolation Note: exact implementation option is subject to the local organisation and country requirements
Location based message delivery	0	0	0	n/a	0: not supported 1: supported
Mission Critical support	1	1	1	n/a	0: non-mission-critical 1: mission-critical
Mission-critical capability support	2	2	2	n/a	specifies what capabilities are available to support mission-critical services. More than one capability may be supported at once 1: Inter-user prioritization 2: Pre-emption 3: Local control

[3] Excludes MCPTT voice communications

ATTRIBUTE NAME	SENSOR DATA	REQUEST / REPONSE[3]	VIDEO DATA	UNIT	COMMENTS
Mission-critical service support	2, 5	2, 5	3	n/a	1: MCPTT 2: MCData 3: MCVideo 4: IOPS 5: MC interworking with LMR systems 6: MC system interconnection and migration Note: where LMR systems are being used in conjunction with 3GPP-based solutions, interworking with LMR systems must be enabled
MMTel Support	0	0	1	n/a	0: not supported 1: supported
Slice QoS parameters	5, 70	70, 80	67, 70	n/a	5G QoS Identifier (5QI)
User data access	0	0	0	n/a	0: Direct internet access 1: Termination in the private network 2: Local traffic (no internet access) Note: direct internet access via proxy with whitelisting / blacklisting



MULTI-AGENCY INCIDENT RESPONSE: VEHICLE CRASH AND CHEMICAL SPILL



The details of this use case can be found in document in [9] section 5.5, summarised as follows:

Incident response from police, fire and rescue and medical personnel to a multi-vehicle crash on a motoroway that includes injuries and a chemical spill from one of the vehicles involved. The focus is on IoT devices and applications that support emergency personnel health and safety, and shared situational awareness between different agencies.

ACTORS

The actors considered in this use case are:

- Firefighters
- Hazmat unit
- Fire department robot
- Law enforcement for traffic management
- Medical personnel

DATA TYPES

The types of data is the same as the house fire incident use case and can be similarly grouped as follows for the different actors listed above:

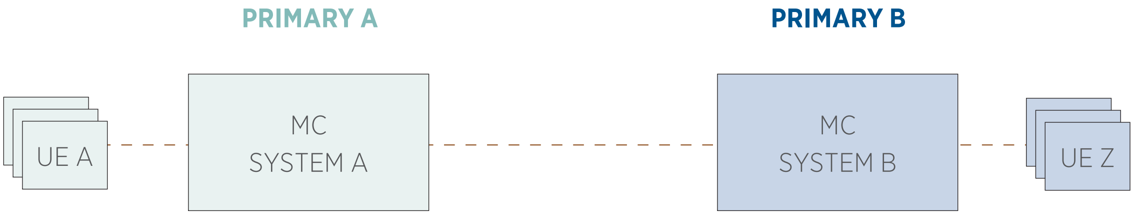
- **Sensor data:** including biometrics, physical trackers and environmental sensors, as described in previous use cases. These sensors may be e.g. body-worn sensors, sensors placed at the incident scene to detect levels of hazardous materials
- **Video data:** thermal imaging, video cameras, lidar
- **Request / response:** type of data triggered by a request or by sending feedback either from an emergency personnel, the incident commander or control room.

INTERCONNECTION AND MIGRATION BETWEEN MISSION CRITICAL SYSTEMS

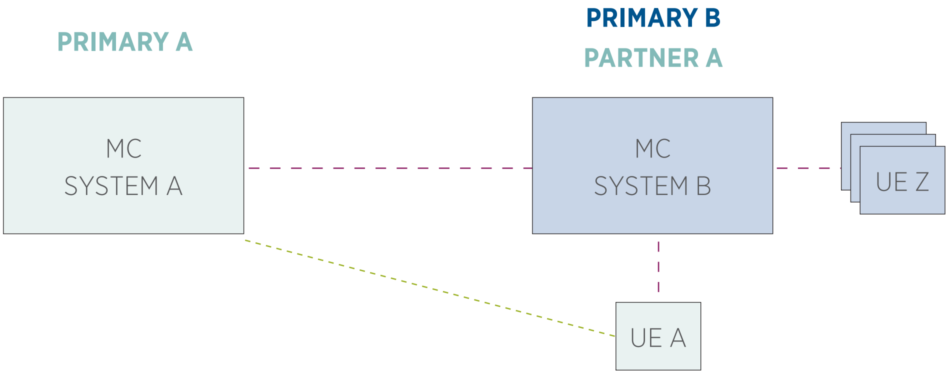
The key difference in this use case compared with other use cases in this document is that there is a requirement for situational awareness information to be shared with multiple agencies in the field, each with their own set of applications and equipment, which may be implemented differently and using different technologies. In such scenarios, interworking with LMR systems will be required, as well as interconnection and migration between 3GPP-based mission critical systems.

'Interconnection' between mission critical systems, where users on different home networks using different systems need to communicate with each other, is illustrated in the following diagram[4]. Here, user A is on its primary system A, which is a combination of home network A and mission critical system A. Likewise, User Z is on its primary system B: home network B and mission critical system B. With interconnection, user A and user Z are enabled to communicate with each other, e.g. to be part of the same group call.

[4] Figure 4.1.2-1 from 3GPP TR 23.781



‘Migration’ between mission critical systems, where users from a different home network and different mission critical system has roamed onto a visited network and is using services offered by a different mission critical system, is shown in the following diagram[5]. Here, user A has migrated to mission critical system B and is receiving services on this system, which enables user A to take part in communications with user Z.



NETWORK ATTRIBUTES

The table below describes the network slicing attributes for three data types described in the previous section:

- Sensor data
- Request / response
- Video data

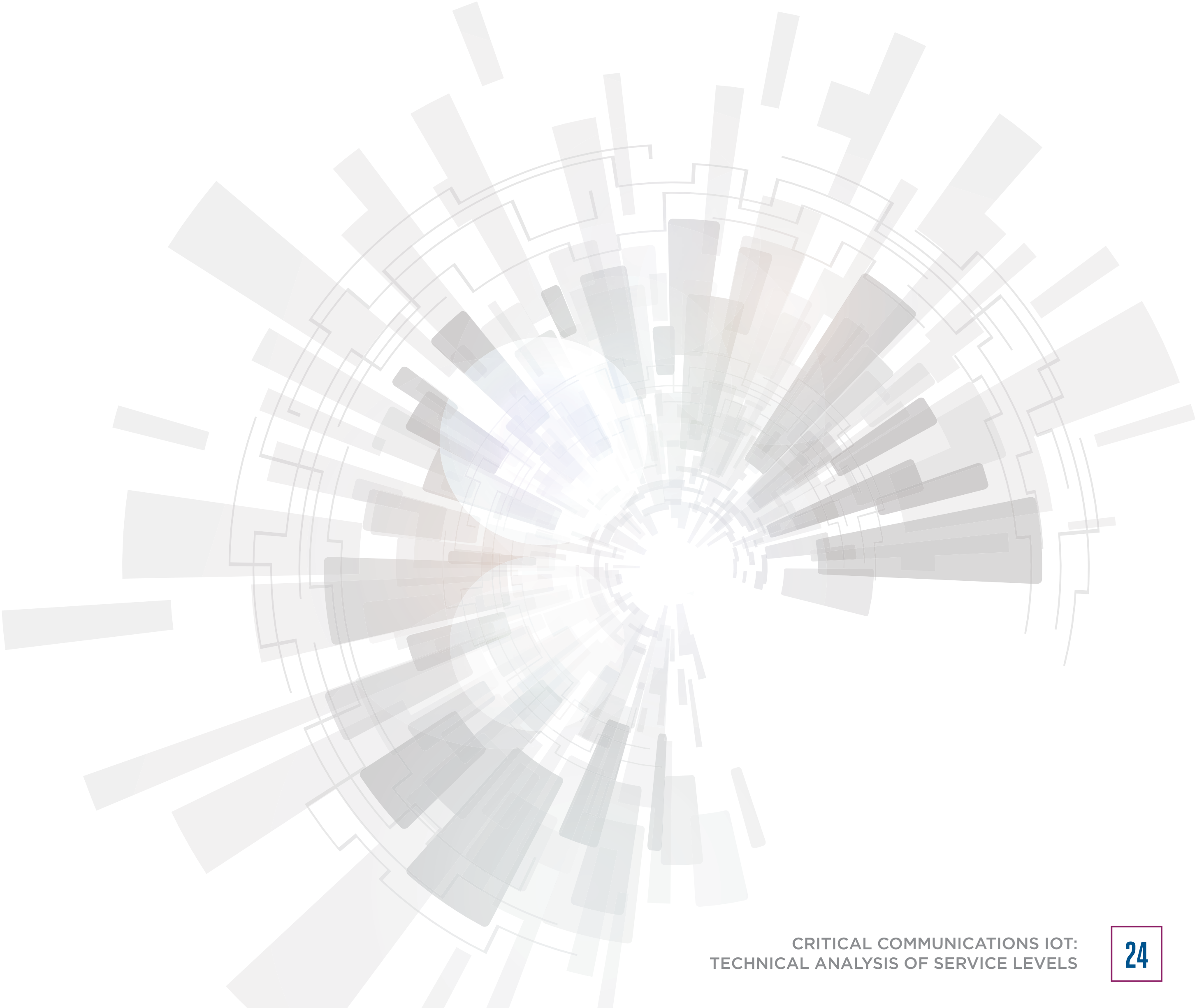
All the attributes are the same as the house fire use case in the previous section, except for attribute ‘Mission-critical service support’ where the the value ‘MC system interconnection and migration’ is added on top of the other values used in the house fire use case.

[5] Figure 4.1.1-1 from 3GPP TR 23.781

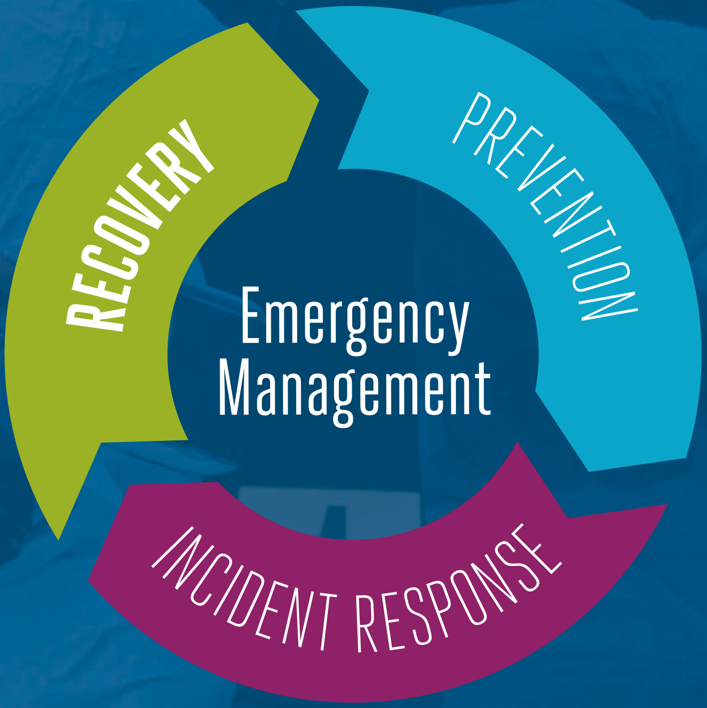
ATTRIBUTE NAME	SENSOR DATA	REQUEST / REPONSE[6]	VIDEO DATA	UNIT	COMMENTS
Deterministic communication	1	0	0	n/a	0: not supported 1: supported Note: where deterministic communications is required, the periodicity value(s) is dependant on the actual use case and not documented here
Downlink throughput per UE	1	2,000	300,000	Kbps	Note: throughput values defined here are based on assumptions made for this specific use case Video: Typically UEs will be either transmitting or receiving video at any one time. However, there will be a mix of UEs, some will be transmitting and others will be receiving.
Uplink throughput per UE	1	50	300,000	Kbps	Note: throughput values defined here are based on assumptions made for this specific use case Video: Typically UEs will be either transmitting or receiving video at any one time. However, there will be a mix of UEs, some will be transmitting and others will be receiving.
Group Communication Support	0	0	2, 3, 4	n/a	0: not available 1: Single Cell Point to Multipoint (SC-PTM) 2: Broadcast/Multicast 3: Broadcast/Multicast + SC-PTM 4: Group communications system enablers (GCSE) Note: this is an example, exact implementation option is subject to the local organisation and country requirements
Isolation Level	2	2	2	n/a	0: No Isolation 1: Physical Isolation 2: Logical Isolation Note: exact implementation option is subject to the local organisation and country requirements
Location based message delivery	0	0	0	n/a	0: not supported 1: supported
Mission Critical support	1	1	1	n/a	0: non-mission-critical 1: mission-critical
Mission-critical capability support	2	2	2	n/a	specifies what capabilities are available to support mission-critical services. More than one capability may be supported at once 1: Inter-user prioritization 2: Pre-emption 3: Local control

[6] Excludes MCPTT voice communications

ATTRIBUTE NAME	SENSOR DATA	REQUEST / REPONSE[6]	VIDEO DATA	UNIT	COMMENTS
Mission-critical service support	2, 5, 6	2, 5, 6	3, 6	n/a	1: MCPTT 2: MCData 3: MCVideo 4: IOPS 5: MC interworking with LMR systems 6: MC system interconnection and migration Note: where LMR systems are being used in conjunction with 3GPP-based solutions, interworking with LMR systems must be enabled
MMTel Support	0	0	1	n/a	0: not supported 1: supported
Slice QoS parameters	5, 70	70, 80	67, 70	n/a	5G QoS Identifier (5QI)
User data access	0	0	0	n/a	0: Direct internet access 1: Termination in the private network 2: Local traffic (no internet access) Note: direct internet access via proxy with whitelisting / blacklisting



RECOVERY PHASE: FORENSIC DATA COLLECTION



In the recovery phase, the focus is on understanding what happened during the incident and to collect any other evidence missed during the initial incident response. Law enforcement and fire and rescue agencies may conduct a detailed search in the vicinity of the incident area in order to reconstruct the events of an incident and to search for more evidence. The process may involve taking new video data of the environment during the post-incident visit for additional video analytics processing e.g. to search for bullets at a crime scene or to search for the source and route of a fire.

The latency requirement in the recovery phase is the most relaxed of the three emergency services phases. It is important to be able to obtain the video data, but high delays can be tolerated. The data rate used is expected to be high due to the amount of video data to be transferred, but typically this is for a short period of time, from a few minutes to a few hours, and covers a limited geographical area around the scene of the incident.

It is possible for the data rate to be reduced if technologies such as edge computing are used for initial processing of the data.

ACTORS

Example of the actors involved in this use case are:

- Fire investigators
- Crime scene investigators
- Forensic personnel

DATA TYPES

The data used in this use case is typically video data with high throughput data of a streaming nature, as described in previous sections.

NETWORK ATTRIBUTES

The following table below describes the network slicing attributes for the video data in this use case.

ATTRIBUTE NAME	VIDEO DATA	UNIT	COMMENTS
Deterministic communication	0	n/a	0: not supported
Downlink throughput per UE		Kbps	Typically UEs will transmitting video and not receiving Note: main focus of the use case is on uplink transmission, so no values are indicated for downlink
Uplink throughput per UE	300,000	Kbps	Typically UEs will transmitting video and not receiving Note: throughput values defined here are an average based on assumptions made for this specific use case
Group Communication Support	0	n/a	0: not available 1: Single Cell Point to Multipoint (SC-PTM) 2: Broadcast/Multicast 3: Broadcast/Multicast + SC-PTM 4: Group communications system enablers (GCSE) Note: no group communications envisaged for this use case

ATTRIBUTE NAME	VIDEO DATA	UNIT	COMMENTS
Isolation Level	2	n/a	0: No Isolation 1: Physical Isolation 2: Logical Isolation Note: exact implementation option is subject to the local organisation and country requirements
Location based message delivery	0	n/a	0: not supported
Mission Critical support	1	n/a	0: non-mission-critical 1: mission-critical
Mission-critical capability support	n/a	n/a	1: Inter-user prioritization 2: Pre-emption 3: Local control
Mission-critical service support	3	n/a	1: MCPTT 2: MCData 3: MCVideo 4: IOPS 5: MC interworking with LMR system 6: MC system interconnection and migration
MMTel Support	1	n/a	0: not supported 1: supported
Slice QoS parameters	6, 8	n/a	5G QoS Identifier (5QI)
User data access	0	n/a	0: Direct internet access 1: Termination in the private network 2: Local traffic (no internet access) Note: direct internet access via proxy with whitelisting / blacklisting

Business Critical use cases

This section covers a few examples of business critical IoT use cases from a couple of industries. Here, an overview of the use cases is provided in order to illustrate how IoT is used in a business critical setting.

There are a number of commonalities in terms of requirements from the public safety community and from the business and enterprise setting. One common goal is for high levels of network reliability, which is important in order to achieve both the business as well as public safety objectives.

Analysis of the performance requirements are not covered here, as they are being investigated by other organisations such as 5G ACIA and 5GAA.

Process Manufacturing[7]

At Shell Pernis, located in the Port of Rotterdam, KPN has deployed an experimental 5G network with a 3.5 GHz frequency band. KPN, Shell, Huawei and other partners have tested industrial 5G-applications with this 5G network at Shell Pernis. With the use of 5G technologies, processes manufacturing can be optimized, industrial maintenance can be better predicted and safety further improved. 5G also enables large-scale deployment of wireless sensors, allowing process manufacturers direct access to relevant digital information from the production environment.

Remote monitoring: The inspection process for gas leaks is critical to the security and safety of industrial facilities. During tests, a mobile inspection robot is connected to the 5G network resulting in a much more accurate and reliable remote control. Safety is improved because humans no longer need to be present to perform inspections on site.

Digital inspections: A fully digital inspection scenario was carried out, using a 5G connected 4K camera on a car that transmitted video images to a machine vision algorithm that is trained to detect corrosion on pipelines. After detection, a plant maintenance task is automatically generated and is send back to the maintenance engineer in the car. Thus, industrial inspections are further digitalized and provide predictive maintenance information, resulting in faster and more efficient inspections and maintenance on the 160,000 km of pipelines at the biggest European refinery, Shell Pernis.

Connected worker: Having all relevant information available to maintenance personnel is key to efficient industrial maintenance. In the tests, engineers were equipped with ruggedized tablet connected to 5G which held augmented reality information, such as temperature or pressure of the process installation. This allows all processes to be fully digitally recorded and shared with all relevant parties.

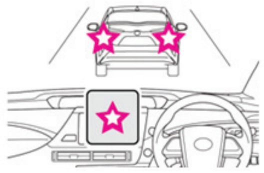
[7] https://overons.kpn/en/news/2018/kpn-shell-and-partners-test-industrial-5g-applications-in-the-port-of-rotterdam

Driving safety[8] [9]

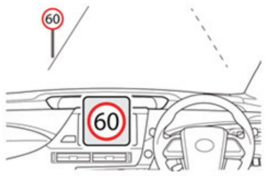
While the rise of autonomous vehicles is drawing much attention, it is unlikely that there will be mass adoption of fully driverless vehicles on public roads for a number of years. As a step in the direction of a driverless future, however, connected and smart vehicles are seeing increased adoption. For example, 75% of cars shipped in 2020 in Australia are likely to be connectivity capable[10] [11]. In the coming years, vehicles' connectivity will be used for more than streaming music and reporting weather: vehicles will be talking to road infrastructure, other vehicles on the road and even pedestrians – very near term possibilities that 5G and IoT can help enable.

In a connected vehicle trial in Australia, operator Telstra partnered with vehicle manufacturer Lexus Australia to deliver a cellular V2X (Vehicle-to-everything) project that establishes the real-world impact of advanced connectivity technologies on improving road safety. Sponsored by road authority VicRoads and the Transport Accident Commission (TAC), the Advanced Connected Vehicles Victoria (ACV2) trial seeks to demonstrate six safety-enhancing use-cases. These use-cases (illustrated below) all involve a human machine interface (HMI) to give warnings of potential hazards to drivers of connected vehicles.

EMERGENCY ELECTRONIC BRAKE LIGHTS (EEBL)

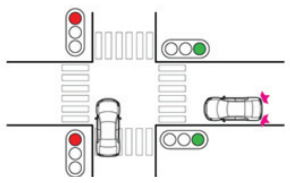


IN-VEHICLE SPEED WARNING



RIGHT TURN ASSIST

RED LIGHT VIOLATOR WARNING



CURVE SPEED WARNING

COOPERATIVE FORWARD COLLISION WARNING

[8] https://exchange.telstra.com.au/making-our-roads-safer-with-connected-vehicles/

[9] http://www.acv2.com.au/

[10] Business Insider Intelligence Connected Car Report (https://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2016-4-29/?r=AU&IR=T)

[11] 5GAA Forecast

These warnings are delivered over Telstra's 4G network, but with a 5G-like experience. As most of the above applications are time-critical (with timely collision warnings being particularly important in a life or death scenario), Telstra has built a low-latency service specifically for the trial. This service sits on top of the 4G network, and uses RAN software features at 4G base stations to provide low latency and high reliability connectivity for vehicle-specific messaging, pre-empting the kind of quality of service 5G could deliver in the years to come. While this service works well for current purposes, 5G (and in particular URLLC) would help with the delivery of this kind of capability at scale.

5G for digital twins in manufacturing industry[12]

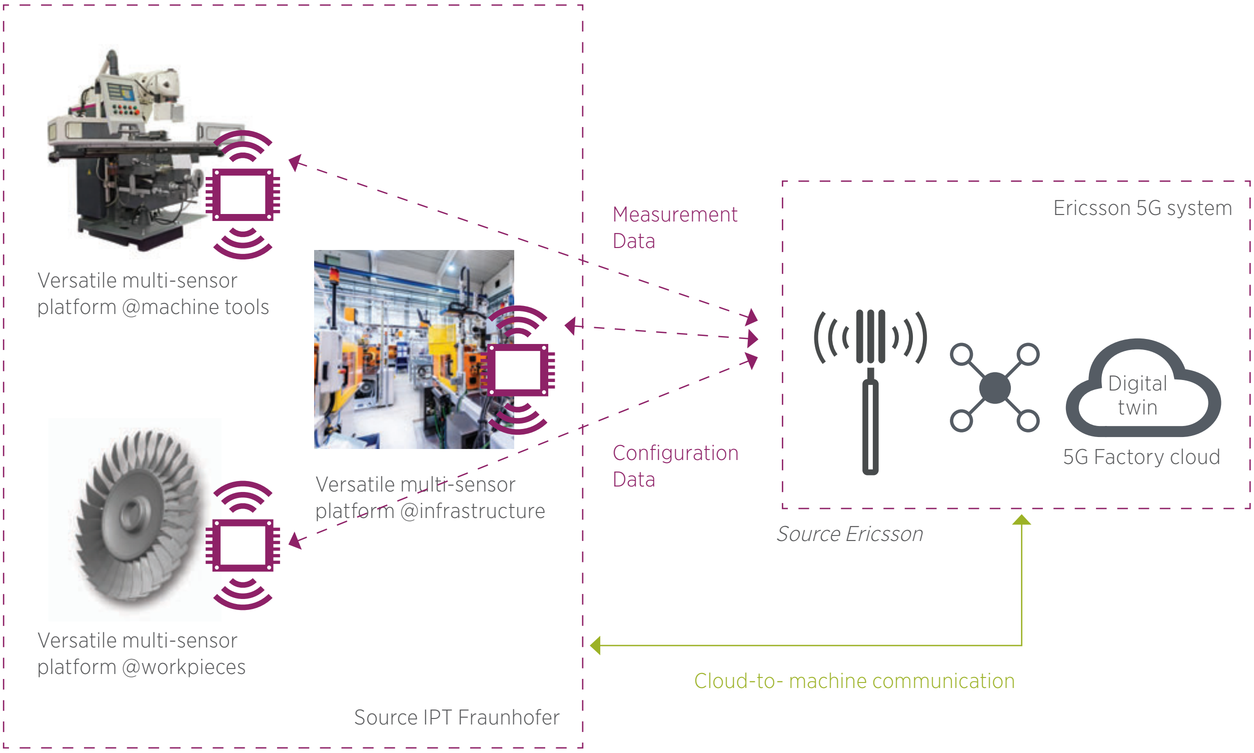
Industry 4.0 benefits from a vast network of wirelessly connected devices enabling continuous, real-time quantitative analysis of all operational processes, material flows and products. The integration of all inputs from multiple sensors into a computational model of the relevant processes gives rise to a digital twin of the production facility, a virtual representation of the critical components and processes of the physical factory.

Such a digital twin may include data on the status, performance levels and conditions of machine tools, an ongoing quantitative assessment of the quality of work pieces and production processes, and an evaluation of the health of the infrastructure. Running synchronously with the production system, it can then be used to optimize the behavior of the real system, test process changes before they are implemented, trigger alerts when something goes awry, and detect and address potential failures before they lead to downtime.

For digital twins to live up to their potential in fast-paced production environments with tightly synchronized processes, they will depend on a combination of ultra-high reliability and low latency. To acquire the necessary data for digital twins, Fraunhofer IPT, Marposs and u-blox are developing a 5G versatile multi-sensor platform for digital twins. Within the context of the 5G-SMART project, the platform will be tested in a trial facility at the Fraunhofer IPT set up by Ericsson. The platform comprises several multi-sensor devices (accelerometer, gyroscope, microphone, temperature, humidity), which are integrated into multiple workpieces at the trial site, where they gather data and feed a digital twin that is hosted in the factory cloud as depicted below.

[12] 5G-SMART, https://5gsmart.eu/, D3.1: Report on industrial shop floor wireless infrastructure, November 2019

Shop Floor –Process and Condition Monitoring


Versatile multi-sensor platform @machine tools
Versatile multi-sensor platform @infrastructure
Versatile multi-sensor platform @workpieces
Source IPT Fraunhofer
Measurement Data
Configuration Data
Ericsson 5G system
Digital twin
5G Factory cloud
Source Ericsson
Cloud-to- machine communication

The Fraunhofer trial is one out of the three trials of 5G-SMART that will assess key performance indicators for 5G connectivity, such as the end-to-end uplink and downlink latencies, the latency variation, the round-trip latency, and the uplink throughput in order to validate 5G performance for advanced manufacturing applications.

6 Conclusions

This document presented an overview of critical communications using IoT technology, with a focus on the mission critical communications perspective, including both business critical and public safety aspects. On the public safety side, the three main phases of emergency management were described, together with a number of typical use cases associated with each of these phases.

A high level overview of quality of service from a 4G and 5G is presented, which is followed by an introduction to 5G network slicing and its related network attributes. Together, these provide the reader with the background to a number of the 5G network slicing attributes and how the attributes apply to the public safety use cases.

From a public safety point of view, the use case were analysed and broken down into various data types that need to be supported by the network, together with an estimation of the data throughput needed for incident responders, such as fire fighters. In addition, the network attributes needed to support the emergency management phases were also described in detail. Taken together, the data types, throughput and network attributes information provide the reader with a comprehensive understanding of the use of IoT technology in the area of critical communications.

The information presented in this document serves as a guideline for mission critical and public safety organisations, to enable such organisations to work together with network operators to define 5G network attributes for their network slice when deploying 5G mission critical IoT services.

7 References

REFERENCE	DESCRIPTION
[1]	GSMA Network 2020: Mission Critical Communications https://www.gsma.com/futurenetworks/wp-content/uploads/2017/03/Network_2020_Mission_critical_communications.pdf
[2]	ISO 22300:2018(en) Security and resilience — Vocabulary https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en
[3]	3GPP TS 23.203, Policy and Charging Control Architecture http://www.3gpp.org/DynaReport/23203.htm
[4]	3GPP TS 23.501, System Architecture for the 5G System; Stage 2 http://www.3gpp.org/DynaReport/23501.htm
[5]	GSMA: An Introduction to Network Slicing https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf
[6]	GSMA The 5g Guide: A Reference For Operators https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf
[7]	3GPP TS 23.468, Group Communication System Enablers for LTE (GCSE_LTE); Stage 2 http://www.3gpp.org/DynaReport/23468.htm
[8]	GSMA NG.116 Generic Network Slice Template https://www.gsma.com/newsroom/all-documents/generic-network-slice-template-v2-0/
[9]	National Public Safety Telecommunications Council (NPSTC) Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes http://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf
[10]	ETSI TR 103 582 v1.1.1 Study of use cases and communications involving IoT devices in provision of emergency situations https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf
[11]	EENA The Internet of Things (IoT) and Emergency Services https://eena.org/wp-content/uploads/2018/11/The-Internet-of-things-and-emergency-services.pdf
[12]	3GPP TS 23.379, Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2 http://www.3gpp.org/DynaReport/23379.htm

REFERENCE	DESCRIPTION
[13]	3GPP TS 23.282, Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2 http://www.3gpp.org/DynaReport/23282.htm
[14]	3GPP TS 23.281, Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2 http://www.3gpp.org/DynaReport/23281.htm
[15]	3GPP TS 23.401, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access http://www.3gpp.org/DynaReport/23401.htm
[16]	3GPP TS 33.401, 3GPP System Architecture Evolution (SAE); Security architecture http://www.3gpp.org/DynaReport/33401.htm
[17]	3GPP TS 23.283, Mission Critical Communication Interworking with Land Mobile Radio Systems http://www.3gpp.org/DynaReport/23283.htm

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA.

About PSC Europe

PSCE is a permanent autonomous organisation working to foster excellence in the development and use of public safety communication and information management systems by consensus building. PSCE is a forum where representatives of public safety practitioners, governmental organisations, industry and research institutes can meet to discuss and exchange ideas and best practices, develop roadmaps and improve the future of public safety communications. Dialogue is facilitated through 2 major conferences per year, and coordination of appropriate policy related activities with and for the European Commission. PSCE brings together those who procure, govern, develop, deliver and use public safety communication solutions across Europe.

For more information, please visit the PSCE website at www.psc-europe.eu.