5G for Defence – 3GPP Capabilities for Military Networks

CONTENTS

This course examines the 3GPP Mission Critical services as the basis for military and defence operational communication over 5G, and the profile a defence user has to put on top of them.

Defence communication over 5G is a commercial standard with a military profile above it: the 5G system as the transport, the 3GPP Mission Critical services as the operational communication layer, and above them what NATO and the nations define for defence use.

It begins with what critical communication demands of a network and what defence demands beyond that, then works through the 3GPP framework, the architecture and the MCX services themselves. It briefly presents the 5G System Architecture: Access Networks and the 5G Core, with the advanced 5G features used for Mission Critical Communication. The course closes with the defence profile: who decides how commercial 5G is used by armed forces, what NATO agreed in STANAG 5665, and what is still missing.

TARGET AUDIENCE

This course is intended for technical professionals involved in the specification, procurement, design, deployment or operation of military communication systems.

PREREQUISITES

Participants are expected to have a technical background. 5G knowledge is helpful but not assumed; the Apis course “5G Standalone Architecture and Features” or equivalent knowledge is strongly recommended. Familiarity with military communication systems is useful but not required.

Introduction to Critical Communication and Defence Services

- Examples of Critical Communication services; service and QoS requirements
- Definition of the defence communication service; military communication needs
- Regulatory considerations: accreditation, standards, spectrum, sovereign control
- Current military systems: combat net radio, software defined radio, satellite, trunks
- Comparison of tactical radio and 5G for defence

Mission Critical/Defence Services in 3GPP

- Defence as a profile of the 3GPP Mission Critical (MC) services
- 3GPP standards and timeline of the MC specifications, Release 12 to Release 20
- Communication components: MCPTT, MCVideo, MCData, Public Warning System
- Comparison of 4G and 5G for MC services; overview of the 3GPP features for MC
- Security features in 3GPP relevant to defence: 5G System and MCX security

Architecture for Mission Critical Services in 3GPP

- Overall MC architecture: MC Service Client and Server, access and core networks
- MC Services Client: MCX, Common Services, HTTP, IMS and ProSe clients
- MC network entities: MCX Server, Common Services Core (CSC), SIP Core/IMS
- CSC functions: Group, Identity, Configuration, Key and Location Management
- Interconnection between national MC systems; federation for coalition operations
- Registration for MCX: 5G, IMS and MCX Service Registration, Group Affiliation

The MCX Services: Push-To-Talk, Video and Data

- Characteristics of Push-To-Talk (PTT): half-duplex, instant, group communication
- Nets, talkgroups and dynamic regrouping
- MCPTT call types: private, group, broadcast, emergency and imminent peril calls
- MCPTT calls: on-network and off-network, pre-established and on-demand

- MCPTT architecture, group call establishment and floor control
- Priority and pre-emption: MCX priority, ARP and 5QI
- Off-network working using Proximity Services (ProSe)
- MCVideo: characteristics, architecture and group call establishment
- MCData: Short Data Service, File Distribution, Data Streaming, IP Connectivity
- MCData architecture and Blue Force Tracking over MCData

Radio Support for MCX in 5G

- MC QoS requirements and the 5G resources used by MCX
- Standardised 5QI values, including the MC 5QIs 65, 67, 69 and 70
- New Radio (NR) features for low latency, high throughput and high reliability
- Network availability: 3GPP terrestrial, Wi-Fi and satellite access
- Wi-Fi access with Access Traffic Steering, Switching and Splitting (ATSSS)
- Non-Terrestrial Networks (NTN): architecture; Earth-fixed, quasi-Earth-fixed and Earth-moving cells

Network Support for MCX in 5G

- Network Slicing: standardised use cases, slice identification (S-NSSAI)
- Defence use of Network Slices; slice template attributes (GSMA NG.116)
- Edge Computing for defence; architecture for edge applications (EDGEAPP)
- Multicast Broadcast Services (MBS): multicast and broadcast sessions, individual and shared delivery, MBS architecture for MC
- Private Networks (Non-Public Networks, NPN): Stand-alone NPN (SNPN), Public Network Integrated NPN (PNI-NPN), private network as a Network Slice
- Examples of dedicated defence networks; deployable private networks
- Resource ownership options; comparison and choice of a deployment model

MCX Enablers in 3GPP

- IP Multimedia Subsystem (IMS) for MCX: session control; IMS registration, capability discovery, session setup and modification, subscription/notification
- ProSe for MCX: direct discovery and communication, UE relays, network support

The Defence Profile: NATO and National

- The need for a defence layer; roles of the NATO bodies, nations and accreditors
- Federated Mission Networking (FMN)
- NATO Standardization Agreements (STANAGs), including STANAG 5665
- NATO work on 5G and national defence 5G programmes
- Defence spectrum: NATO harmonised bands, host-nation clearance
- Coverage from garrison to the tactical edge
- Deployable and mobile cells: on wheels, man-portable, vehicle-mounted, airborne
- Military waveform components; electronic warfare and the 5G waveform
- Classified traffic over commercial technology: Commercial Solutions for Classified (CSfC), cryptography, zero trust
- Sovereignty and the supply chain

References

- 3GPP reference list; NATO, national and industry sources