Technical Report on

5G Network Architecture and Security

A collaborative paper

DCMS Phase 1 5G Testbeds & Trials Programme

December 2018

This paper is the collaborative output of DCMS 5G Testbeds and Trials (5G T&T) [1] Phase 1 Projects AutoAir, 5G RuralFirst, and Worcestershire, as well as 5G Innovation Centre (5GIC). In this paper, the combination of these three testbeds and the 5GIC testbed is referred to as 'the Collaborators'.

Executive Summary

Fifth Generation (5G) testbeds to innovate, deploy, and test 5G networks, platforms, and novel technologies are now being set up around the world. The aim is to verify the inter-operability of new mobile network components and radio equipment and to evaluate the performance of new applications and use cases.

The Third Generation Partnership Project (3GPP) is defining 5G standards to secure the network core, radio and user equipment, which include procedures for user privacy assurance and identity management. Understanding these relationships is essential to build new businesses and to ensure that critical applications can operate safely, fully qualifying and understanding the risks across the entire eco-system. Privacy assurance and identity management procedures also need to be linked to user consent and data handling mechanisms.

The International Telecommunication Union (ITU) vision for 5G outlines use cases with very diverse technical performance and system requirements, requiring mobile networks to interconnect with different non-3GPP network technologies. This cannot be achieved by a single network operator in their own domain. There is a definite need to have network-to-network inter-operability, which must also be secured and trusted. 3GPP has published 5G specifications that define interfaces for inter-network communications, yet further work is necessary to evolve interface functionality, performance and security. To realise seamless inter-operability, effective partnerships are necessary between different network operators and equipment owners, such as transport companies, rural and local communities and authorities, and publicly funded organisations. To achieve end-to-end security, network boundaries need to be secured across all borders.

Inter-connection of 3GPP and non-3GPP networks, new 5G use cases with diverse requirements, new 5G technologies, including evolutionary approaches in the mobile network all add to the complexity of the new platforms. This brings new security vulnerabilities, with a significantly larger attack surface, making it essential to thoroughly evaluate the risks and vulnerabilities, and identify work items to alleviate them. Furthermore, the various challenges to deploy secure 5G networks, whilst meeting the requirements of different 5G use cases, creates a trade-off challenge between network performance and security. The combination of increased network-to-network complexity, end-to-end cross layer system security and critical applications will mean conventional security methods will not be feasible.

New technology will be required to meet these challenges to prevent conventional security approaches compromising the required 5G performance. Context-aware networks and artificial intelligence (AI), which can process context transfer patterns and correlate them with user, device, application, and security context meta-data to make predictive decisions, present the UK with a significant innovation opportunity. This will assist the network to make sure the system set up is one step ahead of the dynamics of the UE behaviour and context, therefore predicting and pre-validating the required end-to-end security and connection in advance of the UE requesting the service.

New innovative 5G platforms are being built by 5G testbed projects in the UK, as part of the DCMS Phase 1 Testbeds and Trials (5G T&T) Programme [1]. The common aim of the testbeds is

to deploy and test 5G networks and evaluate performance of these networks for a variety of use cases. This is a stepping stone to build 5G capability in the UK and strengthen UK's competitive capacity with global players. The testbeds will open up new innovation opportunities and scope for wider small and medium-sized enterprise (SME) involvement, which is necessary economically and to ensure UK success in faster deployment of 5G.

This paper introduces four 5G testbeds in the UK, three of which are built as part of the DCMS Phase 1 5G T&T Programme and begins to evaluate the scope of the security vulnerabilities posed by the complexity of 5G systems. In doing so, the paper's aim is to raise awareness and highlight the need for cross-domain, cross-layer, end-to-end security in 5G. The paper also highlights the areas and need to work on these cross-layer challenges collaboratively across different sectors proposing to use 5G, e.g. standardisation bodies, forums, operators, industry and academia creating the new 5G technologies.

Recommendations

This paper highlights several challenges that need to be addressed if the UK wishes to be a leader in the development and deployment of 5G. In particular, the need for further investment and innovation related to:

1) Cross-layer standards and framework enabling end-to-end security for prioritised critical or vertical segment use cases,
2) A new approach to predict and pre-validate cross-layer user equipment (UE) connections, utilising Artificial Intelligence (AI) and context-aware networking, to ensure 5G performance is not compromised,
3) An organisation that is tasked to help monitor and encourage good security-by-design practice, and set out and document an approach to designing secure 5G networks, applications and services,
4) Standardisation and security tests and trials.

Table of Contents

List of Figures

List of Tables

1 Introduction

The main purpose of 5G is to achieve the goals set out in IMT-2020 [2] of delivering the various 5G use cases, as illustrated in Figure 1, and their performance requirements. The near-future 5G eco-systems should meet these requirements and enable networks of networks in a common approach for 5G infrastructure deployment.

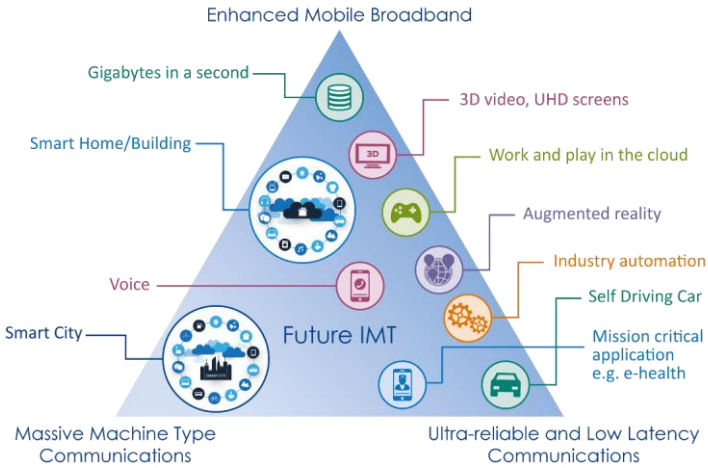

Figure 1. ITU 5G use cases [1].

1.1 Requirements for 5G use cases

ITU has defined the 5G use case categories [2] as *(i)* enhanced mobile broadband (eMBB), *(ii)* ultra-reliable and low latency communications (URLLC), and *(iii)* massive Machine type Communications (mMTC).

3GPP has also identified these use cases, respectively as *(i)* enhanced mobile broadband [3], *(ii)* critical communications [4], and *(iii)* massive Internet of Things (mIoT) [5].

Table 1. Categorisation of 5G use cases by ITU and 3GPP, and their performance goals [2][3][4][5].

Use case category	Performance goals
eMBB	High data rate, low latency
mIoT/mMTC	Ultra-high device density, ultra-low energy consumption
URLLC, critical communications	Ultra-high reliability, low latency, strong security

The quantitative performance requirements of these use cases can be summarised as follows in Table 2.

Table 2. Quantitative performance design goals of 5G use cases[1].

Use Case	Category	Requirement
eMBB	Per connection throughput	1-10 Gbps
	Cell downlink aggregate throughput	20 Gbps
	Cell uplink aggregate throughput	10 Gbps
	Indoor throughput per m^2	10 Mbps per m^2
	Downlink throughput per user	100 Mbps
	Uplink throughput per user	50 Mbps
	User plane latency	4 ms
	Control plane latency	10-20 ms
	Mobility (dense urban)	Up to 30 Km/h
	Mobility (rural)	Up to 500 Km/h
mMTC / mIoT	Number of devices connected per km^2	1 million
URLLC, Critical communications	User plane latency	1 ms
	Control plane latency	10-20 ms
	Reliability	99.999%

Besides these performance requirements, 5G systems are expected to lower network deployment costs, provide perception of increased availability and coverage compared to legacy systems, whilst meeting increased mobility profiles, which are categorised as: stationary (0 km/h), pedestrian/low mobility (up to 10 km/h), vehicular (10-120 km/h), and high-speed (120-500 km/h). The 5G vision cannot be achieved through conventional networking approaches; an unprecedented amount of system innovation, which connects multiple systems, will be required. This will put pressure on network operators and infrastructure providers; therefore, new technologies are required to deliver secure 5G services seamlessly operating across multiple network boundaries, i.e. secure inter-operable networks.

1.2 Security in 5G: A wider scope

To achieve inter-operability, and ensure performance guarantees as outlined above, 5G mobile networks will need to interconnect with legacy networking solutions and various access technologies. This calls for seamless mobility, network management, and performance assurance, requiring technical and commercial engagements between various technology providers. As a result, security of 5G networks, systems, and services is now more challenging

[1] Orchestration of fixed and mobile networks and services is to be envisioned for these use cases, especially for eMBB that has higher bandwidth requirements, which can be addressed with autoscaling and horizontal slicing support. As for URLLC, traffic flows need deterministic quality of service (QoS) support, as well as a highly resilient and secure end-to-end (E2E) system.

than legacy systems, considering the various types of adjunct networks, devices, and services involved. Security mechanisms for 5G systems must therefore meet the following overall requirements:

- *Cross-layer security:* Whilst different security technologies are effective in their respective domains, a unified framework is necessary to coordinate these technologies over different security layers. Within this document, these layers are defined as:
    - Services, Applications, and Use Cases,
    - Users and Things
    - Inter-networking
    - 5G Mobile Network and Virtualisation Systems
    - Physical Infrastructure

  This is to ensure that a gap in one layer does not nullify the benefits gained in others. See Section 3.4 for more information.
- *End-to-end security:* As in legacy systems, it is fundamental to have security assurance in the communication paths between user devices and the termination point of the core network, including radio access and transport network backbone. New challenges arise due to the distributed and highly flexible nature of 5G systems and networks.
- *Cross-domain security:* Inter-operability brings its own challenges arising from coexistence of multiple domains of authority, including networks, services, and equipment. With new players now involved in 5G systems, such as virtualisation technology vendors and providers, and due to the wide range of use cases, each with unique and differing performance requirements, alignment and cooperation is needed between parties to ensure that integrated solutions are inherently secure, and cross-layer security is also ensured across multiple domains. It must be noted that cross-domain security is not equivalent to cross-layer security; i.e. each domain needs to implement cross-layer security and can operate with other domains securely.
- *Secure-by-design:* Security must be part of the design process and security solutions must be deployed early on. Such an approach minimises potential gaps which may not be easy to address after the system is fully deployed and functional.

1.3 Enabling technologies for 5G goals

To achieve 5G technical goals, networks need to be highly flexible, scalable, and programmable. Several recent technologies, e.g. Software Defined Networking (SDN) [6], Network Function Virtualisation (NFV) [7][8], Multi-access Edge Computing (MEC), and Distributed Core and Network Slicing, as outlined by 3GPP [9], have various features and benefits to achieve these goals. These technologies are envisioned to be an integral part of future mobile networks, supporting a large set of existing and new use cases, enabling a wide-range of services offered to users [10]. Furthermore, these technologies allow software programmable solutions, when possible, so that hardware equipment can be repurposed and dynamically programmed

according to the use case and service. In testbed terms, this programmability will enable the testbeds to evolve for future research and development needs.

- **Software Defined Networking (SDN)** [6] allows for dynamic programmability (for example, reconfiguring switches or routers of the network) to be transitioned to separate data and control planes, with a centralised controller.
- **Network Function Virtualisation (NFV)** [7][8] allows multiple network configurations including distributed IP address allocation and firewalling, and network scaling based on demand.
- **Multi-access Edge Computing (MEC)** (aka Mobile Edge Computing) [11] brings the data closer to the end-user, moving the computing and storage functions towards the edge of the network. This reduces not only latency but also the data volume handled by the core and the network backbone and will therefore bring performance benefits. New applications and services are also possible with edge computing.
- **Distributed Core Network** [12] brings the ability to move core network functions to those places where there is the greatest user demand. Distributing functions (such as authentication) brings performance benefits, reducing latency and allowing for ultra-low-latency communications.
- **Network Slicing** [13] allows for multiple virtual networks to be operated over a single, shared physical infrastructure. Network slicing spans multiple layers of the network, from the radio interfaces through to the Layer 2 virtual local area network (VLAN) to Layer 3 virtual routing and forwarding.

The above technologies require enablers in place, such as low-latency fibre connectivity, end-to-end network monitoring, visualisation and data warehousing.

On the other hand, full integration of these technologies must be in place, and such integration must be extensively tested for its reliability, performance and manageability. The new technologies also bring about new challenges, especially from a security perspective. New infrastructure, systems and devices pose new threats to system integrity.

1.4 DCMS 5G Testbeds and Trials (5G T&T) Phase 1 Projects

The three DCMS 5G Testbeds and Trials (5G T&T) [1] Phase 1 Projects (AutoAir, 5G RuralFirst, Worcestershire) have collaboratively worked together to create this paper. In this paper, the combination of these three testbeds and the 5GIC testbed is referred to as 'the Collaborators'.

The 5G testbeds being built by the Collaborators have the above powerful 5G technologies embedded into the systems being deployed. These systems will provide the UK with a significant advantage in the global race for 5G and will place the UK at the forefront of this cutting-edge technology. Further automation, security, resilience, and reliability improvements during the course of the project will further enhance the UK leadership position by differentiating and leveraging UK strengths on Security, System Innovation and Wireless R&D.

The full potential of 5G will not be realised without a mechanism or framework to securely connect disparate systems and assets owned by different organisations and/or consumers. The Collaborators are developing inter-connections that provide inter-operability between networks. The longer-term vision of the Collaborators is to encourage common approaches

through standards to build and scale inter-connected 5G networks to realise multiple end-to-end systems interacting and seamlessly setting up connections for new use cases and services running over multiple organisational boundaries and systems to deploy services in real time.

Adopting common approaches will promote rapid and easy expansion of the 5G capability in the UK to strengthen UK's competitive capacity with global players, with many more use cases to be provided by prospective partner sites as the Collaborators' testbeds evolve. This will open up opportunities for wider micro and SME involvement, necessary for UK success economically as well as faster deployment of 5G.

1.5 Paper Aim and Scope

This paper presents the architectures of the Collaborators' testbeds built by the three projects of the DCMS Testbeds and Trials Phase 1 Programme. Including the 5GIC testbed, the Collaborators' have four testbeds in the UK, supported by several companies and universities.

The paper presents a review of potential gaps and issues that arise in 5G networks and highlights areas to work on collaboratively across standardisation bodies, the industry and academia. Towards this, the paper evaluates the scope of the security vulnerabilities posed by the complexity of 5G systems, and notes the need for cross-domain, cross-layer, end-to-end security in 5G.

The paper is aimed to set the initial baselines for security implementation and tests for 5G networks, not only for the testbeds that are being built by the Collaborators, but for similar networks, trials and testbeds around the world targeting 5G system(s) integration. By considering different security layers, and 5G-specific new features, the paper emphasises the need for end-to-end security as an integral part of 5G networks, which must be in place by design.

The rest of the paper is organised as follows. Firstly, the Collaborators' testbed architectures are introduced in Section 2, including the inter-connection architecture and summary of component testbed structures. Then, Section 3 introduces different security layers in the system and presents the Collaborators' analysis of potential issues related to security. Section 3.5 outlines a set of guidelines and conclusions drawn from building the 5G Testbeds and ways forward to fill the gaps towards end-to-end (E2E) security assurance. Finally, Section 4 provides the appendices on component testbed details, 3GPP 5G security and its features, and a number of standards developing organisations and industry forums working on 5G security.

2 Network Architecture Design

The Collaborators' testbeds have been built to realise a distributed network as well as inter-networking between multiple network domains, which is crucial to achieve for 5G networks of the near future, in support of a wide range of applications. The four testbeds hosted at multiple locations across the UK are:

Table 3. Collaborators' testbeds.

Testbed	Key Technologies	Location
5G Innovation Centre (5GIC)	5GICE – Exchange capability to connect multiple test beds, powered by SDN, NFV, and MANO, Fully virtualised and orchestrated 5G Core Network, supporting Control and User Plane Separation (CUPS), and mobile edge computing (MEC), remote user plane function (UPF), Network Slicing based on Flat Distributed Cloud Architecture (FDC), Outdoor and indoor RAN, including 5G NR and LTE-A eNodeB, Distributed Denial of Service (DDoS) protection, Middleware for deployment of network services across multiple component testbed virtualisation systems.	Guildford, Surrey
AutoAir	Multiple Transport Modes and Use Cases, including high speed mobility Connected Autonomous Vehicles (CAV) millimetre Wave (mmWave) mesh backhauling Mobile Edge Computing for Vehicle to Infrastructure (V2I) use cases 5G New Radio, 3.5GHz, 700MHz	Millbrook
Worcestershire	Industry 4.0 Use Cases over multiple test beds sites, Security testing and analysis, Outdoor and indoor RAN, including 5G NR and LTE-A eNodeB, supporting 3GPP non-stand-alone (NSA) 5G architecture Mobile Edge Computing (MEC) Augmented Reality (AR)	Worcestershire
5G RuralFirst (5GRF)	5G Core supporting NSA & SA architecture, CUPS, MEC, remote UPF Shared spectrum management, 4G, 5G, Lora, NB-IoT, WiFi, 5GHz, 3.5GHz, 26GHz, 700MHz Light-Fidelity (LiFi) and radio backhaul, fixed wireless access, low cost radio, community managed radio Crop management, drones, tractors, spectral imaging Legionella monitoring, AR veterinary, cattle farming Tourism, connected mass transport, 5G to ferries, 5G radio broadcast mode, IoT sensors grid management, windfarm weather detection	Orkney, Shropshire, Somerset

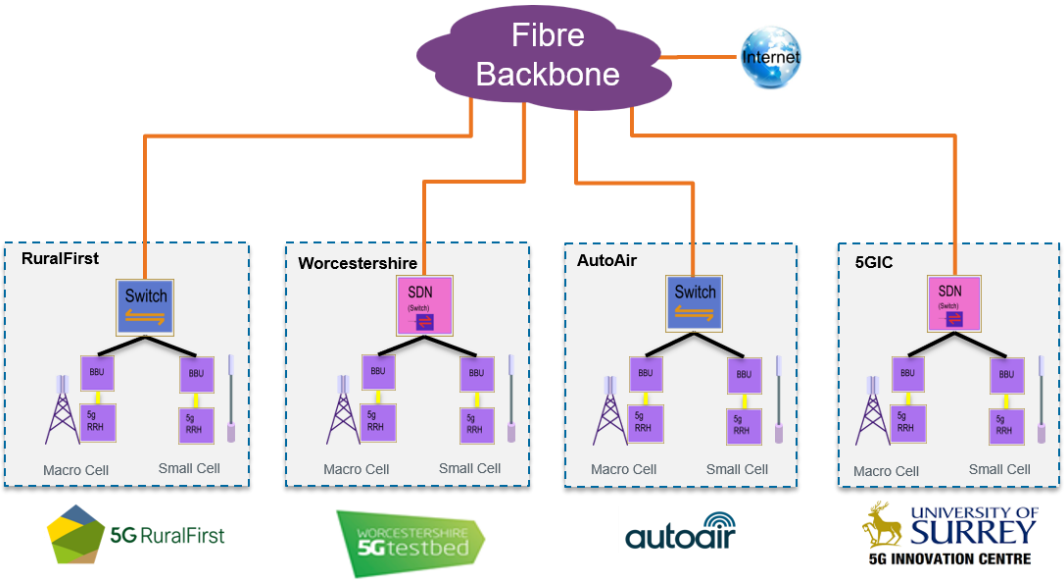

Figure 2: The Collaborators' logical connectivity architecture.

The architecture supports future expansion, and follows enabler principles, such as the use of standard communication interfaces as well as local administrative and operational control of partner testbeds, whilst also providing standardised means for partner testbeds to expose their preferred capabilities. The UK-wide expansion is envisioned to support many more sites across the country at different levels of interconnections, for example at RAN, or RAN and Core or just at application level.

2.1 Testbeds

The Collaborators have four testbeds: Worcestershire consisting of five partner sites, AutoAir in Millbrook, 5G RuralFirst with rural locations across the UK, and 5G Innovation Centre in University of Surrey. Each testbed supports a variety of technologies, ranging from core networks to radio access.

2.1.1. Worcestershire

The Worcestershire testbed consists of five local partner sites with various use cases, such as industrial monitoring and E2E security. To support E2E 5G network operations, the Worcestershire testbed has a dense deployment of the 5G RAN. The RAN systems in the Worcestershire testbed are in general designed to be capable of supporting both 5G and 4G connectivity, and there are several radio frequencies used for 4G and 5G.

The testbed follows the concept of a distributed mobile core network and has data centres to host multi-access edge computing (MEC) services which user devices can interact with via secure local breakout points at partner sites. This enables MEC based services in addition to the testbed's connectivity to the 5G Core hosted at the 5GIC testbed, providing Internet services through its virtual mobile core network slices.

Pre-defined use cases have been determined by Worcestershire testbed partners, which will allow measured testing of the capabilities and risks posed by the 5G infrastructure. The testbed will enable testing of *(i)* communication capabilities, *(ii)* application security, and *(iii)* communications security (i.e. over-the-air and 5G backhaul connections) within a live real-time 5G communications environment.

2.1.2. 5G RuralFirst

The 5G RuralFirst test network spans across four sites in the UK: Somerset, Shropshire, Glasgow, and Orkney Islands.

The Somerset site houses radios delivering on cattle farming use cases including cattle collars and veterinary augmented reality.

The Shropshire site houses a series of agriculture technology use case experiments which leverage MEC, remote user plane nodes, local artificial intelligence, farm machinery automation, and drone and aeroplane crop surveillance.

Orkney Islands host rural community broadband using community low cost radio, community managed radio, LiFi & 5G fixed wireless access, 5G broadcast radio, as well as numerous IoT use cases designed to incrementally build the case for rural connectivity.

The DataVita site in Glasgow houses the cloud core, automation machines, and inter-connect points to other cloud applications including spectrum data bases.

2.1.3. AutoAir

The Millbrook AutoAir 5G-enabled testbed, enabling transport use cases, such as connected autonomous vehicles (CAV), is one of two testbeds of the AutoAir project which has been built to develop connected transport technologies and allow access to all its players. This testbed has a comprehensive infrastructure that includes a fibre backbone, 59 small cell base station sites, and three MEC appliances for local breakout.

This testbed connects to the 5GIC testbed via low bandwidth connectivity for control plane only since all the user traffic is locally carried within the nodes in Millbrook. Connectivity between the nodes in Millbrook is provided using gigabit ethernet connections and an assigned virtual LAN used for mobile traffic over the 3GPP S1 interface [9].

The architecture is logically split into Core and Edge (MEC) networks with Operations and Maintenance (OAM) capabilities as well as a series of V2I CAV functionality. The implementation of Edge network (MEC) functionality is achieved through the separation of Control and User Plane (CUPS). The architecture also offers eNodeB splitting through an *S1 splitter* to enable neutral host capability and allow different operators to access different slices of the network.

The testbed will be operational by January 2019 and will be jointly operated by the network operator Dense-Air, 5GIC, and Millbrook. Section 4.2.1 provides more detail on the AutoAir testbed.

2.1.4. 5GIC

The 5G Innovation Centre (5GIC) [14] testbed has dedicated 10Gbps ports to connect external sites with an aggregate connection capacity of 100 Gbps. The testbed hosts a data centre which has an NFV virtualisation system, an NFV MANO orchestration system, and a Middleware for deployment of virtual network services across multiple testbeds. The 5GIC testbed has integrated-SDN for interconnecting the other component testbeds to its virtualisation system. Multiple virtual network slices run as network services, each for different 3GPP use cases, supporting network slicing. Please see Section 4.2 for more detail. The testbed provides both 4G (LTE EPC) and 5G core network slices.

2.2 3GPP Network Architecture

5G networks will not be possible without a mechanism or framework for operators to be able to commercialise the various sets of features and services. 3GPP has published various specifications for 5G, i.e. Release 15 and Release 16 documents.

The 5G system architecture published by 3GPP in the technical specification document TS 23.501 [9] has a modular structure, as shown in Figure 3, in which components of the core network can be instantiated multiple times to support virtualisation technologies and network slicing. The architecture is driven by the motivation to remove the data overlay that has been traditionally used in previous generations of mobile networks. Architectural changes were needed to enable serving a large number of devices (massive IoT), generating intermittent traffic, whilst dealing with high level of video traffic over mobile networks anticipated for 5G networks. The requirement for user plane E2E latency to be less than 5ms also necessitated architectural change, so that only related network functions would be involved for individual data sessions, rather the complete core network over heavy connections. Reduced latency requirements also stem from 5G support for some use cases such as autonomous vehicles. 5G in general is expected to have 5-10 times lower latency than 4G.

One of the main features of the architecture is the separation of control and user plane operations, which effectively means user plane functions (UPF) can be dynamically programmed by a control plane entity, i.e. the session management function (SMF). This enables central programmability of multiple UPFs which can be distributed in a wide area topology and instantiated on demand. Such UPF components can also be chained via the N9 interface, to form a series of user plane processing entities, each of which can be dedicated to performing specific operations. The rest of the control plane operations have been centralised at the access management function (AMF), making possible to have quick establishment and modification of new bearers, and as easier context management point in the core network.

To support network slicing operations, a specific component called the network slice selection function (NSSF) has been defined to work with the control plane function AMF, which assists in network slicing operations to allocate network slices to user traffic flows.

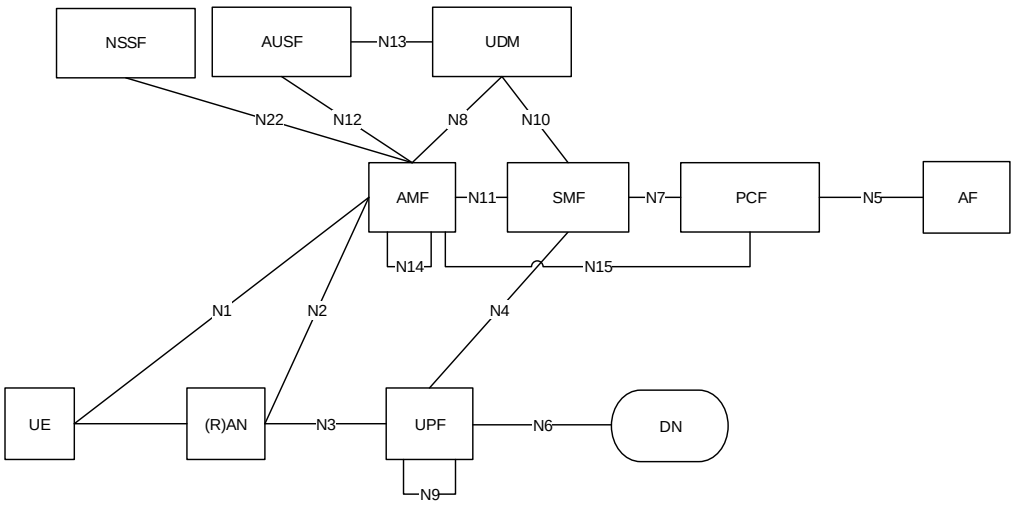

Figure 3. 3GPP 5G system architecture for non-roaming cases [9].

A separate specification, TS 23.502 [15], defines the procedures for the 5G System. The 5G system architecture is service based. REST API [16] based implementation of function interfaces enables interaction of control plane functions much easier than what previous generations could support. As shown at the top of Figure 4, control plane functions can communicate using HTTP messages, with REST API calls to each other on their well-defined interfaces. This architecture makes development of the 5G core far more modular as compared to legacy systems and supports different network slicing strategies via mobile core network orchestration. New functions called the network exposure function (NEF) and the network repository function (NRF) make it possible for newly instantiated or existing functions to discover others, so that a communication session can be established among them dynamically.

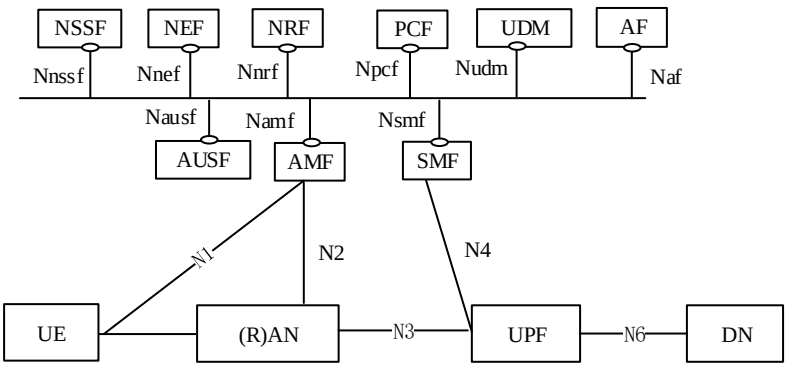

Figure 4. 3GPP 5G system architecture for service-based interfaces [9].

The service-based architecture helps to define modular components, effectively eliminating large data pipes, and reducing system complexity.

3 Security

Various potential problems and challenges related with 5G networks can be identified today, based on experiences with legacy mobile systems, and the added complexity with various 5G technologies that will now be part of mobile systems for 5G. Determining these problems requires understanding the structure and function of the 5G system (which consists of the mobile network, the access technologies, devices and services), as the challenges are intrinsically linked to the system itself. Furthermore, as part of the whole 5G system, it is necessary to *(i)* clearly understand the purpose of different technologies used in the network, and *(ii)* fully consider the architecture of 5G networks, as architecture must be coupled with security because otherwise there would be more vulnerability. This system understanding allows security professionals to identify processes and components within the system without which the network would not achieve its purpose. In this section, the vulnerabilities of the new 5G system have been assessed based on the principals of information assurance, information security, and cyber security.

Whilst building the testbeds, the Collaborators are investigating the security challenges necessary to ensure longer term *Security by Design*[2] approaches. This involves applying security mechanisms where it is practical and available (standardised) and identifying the gaps to address E2E security for future 5G systems. This includes the design team closely cooperating with technical security experts. It also involves soliciting technical security architecture and information assurance opinions before each major design decision. Security-by-design enables both the design team, security organisations and users to be aware of vulnerabilities, thus ensuring full understanding of risks, incorporated controls, mitigations, and vulnerabilities. This in turn enables users and operators to manage risk more effectively and improves security testing.

3.1 Security Principles

In a security context, the following must be taken into account as goals of the complete 5G system to deliver to its providers and users.

- **Anonymity:** Anonymity is used in mobile networks to prevent an attacker from being able to identify individual users. Anonymity is also important in preventing traffic monitoring and traffic analysis by adversaries, including through infiltration of the Core or the RAN. It prevents an attacker from being able to either monitor their communications and/or being able to track their movements.
- **Confidentiality:** Mobile networks provide encryption on the air interface between the UE and the base station to prevent any attacker from eavesdropping on any communication to and from the UE.

[2] *Security-by design* - The phrase entered the security vernacular a few years ago in recognition of the need for requirement managers, system designers, and project teams to consider security requirements upfront in design decisions. Changes in technology and the timing of Information Assurance accreditation in project life-cycles were creating ever increasing challenges that needed to be addressed early in system and project delivery.

- **Verifiable Identity:** In order to prevent an attacker from impersonating a user in order to fraudulently obtain services for free, mobile networks challenge each UE to verify its identity.
- **Safety:** The 5G mobile network is expected to feature prominently in the safety of critical national infrastructure control systems.
- **Availability:** Mobile networks rely upon the network architecture being designed in such a way to ensure and improve availability across the network. For instance, the evolution of the air interface has enabled higher data rates. Furthermore, improvements in connectivity infrastructure also enable higher data rates and increased reliability for successful rates of transfer across the network. It must be noted that network performance and its availability to users may have trade-offs with the above security goals. Hence, a secure system must not compromise network performance, and similarly, providing a highly available network should not mean underestimating security considerations.
- **Physical and Software:** Security is not just about encrypting data streams, but also about physical deployment of equipment. Device and equipment location, type of equipment, and type of services running on the equipment are all parts of the complete system. For instance, MEC servers must be located at secure locations, just as the core network data centres are.
- **Up-to-date system:** The system must be loaded with the latest security solutions, considering different layers of the OSI protocol stack. This includes physical equipment security solutions, all the way up to applications and services. For instance, distributed denial-of-service (DDoS) attacks should be blocked at anti-DDoS systems in place, especially at network interconnection points.

3.2 Risk Owners

It must be noted that decisions about how to respond to security challenges need to recognise that a completely secure network will never be possible. Furthermore, some security controls have an associated cost, either in performance or monetary cost. Hence, it is necessary to take prioritised actions when the complete system is considered. On the other hand, knowing where to prioritise the security activity for a testbed network is not trivial.

According to past practice and experience in information security and cyber security, it is essential to first address the issues related with and affecting those persons and/or organization who have the greatest amount to lose should the system lose integrity, not be available, or not be confidential. In the security world, these individuals and organisations are referred to as the 'Risk Owners'. In the scope of this paper, the main risk owners have been identified as *(i)* the Operators, i.e. those who run the network service on behalf of others, and *(ii)* the Users as the *Risk Owners*.

Risk owners can be considered to fall into example categories as shown in Figure 5. Here, higher levels in the pyramid correspond to a conceptually higher risk per user as compared to those in the lower layers of the pyramid[3]. In contrast, the appetite for risk (aka *Risk Appetite*) conceptually increases further down the pyramid, as the number of users affected by a security

3

breach increases, i.e. the greater the number of users the greater the impact there would be, should something go wrong.

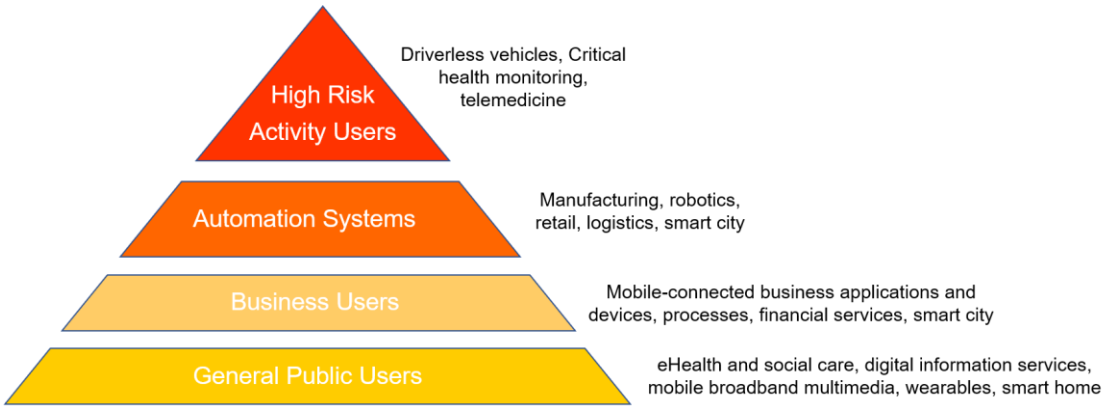

Figure 5. Indicative risk owner categorisation in 5G networks, with examples of use cases for each category listed [4].

While meeting the security requirements of these 5G use case categories, the requirements of the main stakeholders of 5G networks and services, as listed in Table 4, must be taken into account. This provides an overall guideline on how to prioritise different strategies that may potentially conflict, such as higher performance vs more stringent security assurance. It must be noted that different use cases may have different factors in place regarding what different stakeholders prioritise the most as their requirements.

Table 4. Stakeholders of 5G networks and services.

Stakeholders	Main requirements
Service providers, including Cloud and Infrastructure (as a Service)	Availability, reliability, resiliency and security. Service level agreements
Network operators and vendors	Revenue and brand protection, licensing and compliance, data confidentiality, service level agreements
National agencies	Protection of national infrastructure, development of economies, law enforcement, emergency services
Businesses, consumers	Data privacy protection, Performance (Quality of Experience)

[4] The figure illustrates conceptually expected risk appetite as layers of 5G service users, i.e. increase in per-user risk levels higher up the pyramid; nevertheless, no definitive conclusion can be drawn, since there may be users at higher risk in specific use cases, even though lower layers of the pyramid in general are expected to fall in lower risk levels.

3.3 Trials and Testing

It is important to look at the Risk Owners and Risk Appetites in the context of testing and trialling. In order to get long-term benefits out of the testbeds and trials work carried out, it is important to perform a brief assessment of each technology deployed in the testbeds against the full set of security principles.

In each technology trial, each security principle should be assessed to see if its requirements have been met or not. This is necessary to plan the next steps to be taken, i.e. decisions (as broadly categorised in Table 5) can then be made as to how to move forward with the technology that has been testbed.

Table 5. Tests and trials of new technology for compliance with security principles.

Test Decision	Security Principle Requirements have been met?	Risk Level	Way Forward
PASSED and EXTENDABLE	Yes	N/A	Can be applied to future examples of this technology or use case. Lessons learnt, and quantitative findings can be published or taken to standards developing organisations as input.
NEEDS TEST FOR EACH SCENARIO	Yes	Low	The technique does not extend to wider situations. Should be subject to further trialling or testing in later iterations.
NOT VERIFIED	No	Low	The principle should be the subject of further investigation.
REJECTED	No	Medium / High	Urgent action is required to address this risk during the lifespan of the trial. This point would be used only where a trial was using real and live data on systems that were not isolated from the public Internet.

The technologies to be tested may be associated with a specific 5G use case or a set of 5G use cases, or they may be generic enough to applicable to any use case. Besides trials targeting specific technologies, it is also necessary to have 'security-specific' trials, i.e. trials which consider a security principle separate from any particular use case.

3.4 Security Layer and Issues

In an integrated 5G eco-system that consists of multiple sites, including RAN, mobile core networks, and non-3GPP access networks, with different types of user devices and things that are connected to the eco-system, there are several *security layers* of the system that need to be analysed from a security point of view. The Collaborators have identified a number of security layers, where different sorts of security issues may potentially arise, and need to be addressed for any 5G network.

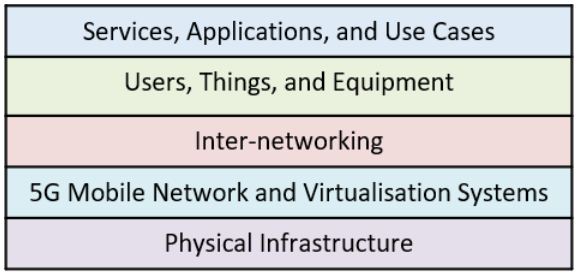

Figure 6. Security layers in a 5G system.

Common to each of the above layers is the increase in *information surface area*. Each layer has increased potential surface area for an attacker when compared to the systems and sub-systems deployed in 4G. Each brings more ways in which the purpose/performance of the 5G network could be undermined. The significance of each (to undermining the integrity and availability of the network) is, however, not equal. Prioritisation of security actions is therefore paramount in bringing effective security to 5G networks.

To analyse different areas where security issues may arise in 5G networks, it is helpful to consider a *security matrix*, which covers the core network, radio access network, transport network and IT infrastructure, user equipment, and applications as services. This is summarised in Table 6, where the five security layers that are depicted in Figure 6 are listed with a number of vulnerability topics noted for each. Each topic is then marked for multiple challenge areas of the 5G networks. The list is not exclusive and is likely to be extended/refined during the course of the DCMS 5G T&T programme, when new potential threats and issues are identified.

Table 6. Security matrix of potential vulnerabilities in 5G networks. (HW: Hardware, SW: Software, SYS: System)

5G PLATFORM SECURITY MATRIX		Affected Areas											
Security Layer	Vulnerability Topic	Radio Network and Air Interface			Mobile Core Network			Transport Network (Backhaul and Fronthaul connectivity)			User Equipment, Device		
		HW	SW	SYS	HW	SW	SYS	HW	SW	SYS	HW	SW	SYS
Services, Applications, and Use Cases	QoS	X	X	X	X	X	X	X	X	X			
	Access rights to network slices	X	X	X	X	X	X	X	X	X			
	Vertical use cases											X	X
	Data confidentiality	X	X	X	X	X	X	X	X	X	X	X	X
	Service and application genuineness, safety, and reliability										X	X	X
	Edge computing and service vulnerability				X	X		X	X				
Users and Things	Device and connection genuineness		X	X		X	X				X	X	X
	Resource limitation of M2M devices										X	X	X
	Device identification for M2M and IoT					X	X						
Inter-networking	Operator models			X			X			X			
	Distributed core				X	X	X						
	Use of various RAN technologies	X	X	X		X	X	X	X	X			
	Separate ownership of RAN for rural and enterprise use cases	X	X	X		X	X	X	X	X			
5G Mobile Network and Virtualisation Systems	Legacy core network vulnerabilities			X			X			X			
	Functional split in the new RAN	X	X	X									
	Software-based operations						X						
	Multi-attribute context authentication					X	X				X	X	X
	Multi-network latency				X			X					
	Network slicing				X	X	X	X	X	X			
	System restoration after failover						X						
Physical Infrastructure	NFV and SDN controllers					X		X	X				
	5G new radio and RAN	X	X	X									
	Active Antenna Management		X	X									
	Commodity hardware vulnerabilities	X			X			X					
	Hardware performance deterioration							X		X			
	Physical Security of base stations, computing systems, and core networks	X		X	X		X	X		X			

In the following, the vulnerabilities listed in Table 6 are briefly explained for each of the five security layers.

3.4.1. Services and applications

The Services and Applications layer involves any application that runs on 5G network(s) eco-system, which can be referred to in a variety of terms, such as User Equipment (UE), users, devices, systems, individual customers, business partners, business customers, third party networks, etc.

Typically, services and applications run on the top layer of the OSI networking stack model. From a security point of view, it is relevant to analyse the interaction of a service/application with *(i)* other services/applications, *(ii)* devices it runs on, *(iii)* the networks that carry the messages generated by or intended for the service/application, *(iv)* the organisational boundaries that the service/application covers or deals with, and *(v)* the infrastructure itself.

Typical security issues involve the use of services, i.e. what the service does, who uses it, and how it affects the system. There are other considerations as well, which can be listed as follows:

- ***Quality of service (QoS)***

  Critical communications use cases will require stringent QoS guarantees in 5G. This requires a robust and secure design, especially for URLLC and mMTC.

  Each network slice in 5G will have a specific set of QoS parameters that define the services that will be associated with that network service. User and device context in 5G must have high granularity, so that efficient decisions can be made regarding allocation of network slices to users and controlling access to running slices by users and devices.

- ***Access rights to network slices***

  Since many services in 5G will run as a network slice, user and/or device access rights to these services, and hence the slices, must be controlled so that the slices cannot be penetrated without permission. This is particularly relevant to network slices running critical applications.

  A single logical instance of a protocol stack layer handles multiple flows related to multiple devices, hence access rights must be carefully managed.

- ***Vertical use cases***

  The level of integration and interworking that is required for applications and services to comply with vertical use case requirements needs to be determined.

  The multiple ways in which applications for users and devices, e.g. Internet of Things devices, Driverless Cars, Smart Home devices, Industrial Control Systems, or Smart Cities, can be configured to operate across the network may create security challenges.

  Among others, financial services and medical/healthcare information services are perhaps two highly challenging areas. Data security, privacy, integrity, and compliance to regulations are all difficult aspects that are fundamental to these verticals.

- ***Data confidentiality***

  From a user point of view, one of the most critical requirements is to ensure that data confidentiality can be assured. In other words, the end-to-end risk appetite of users must be taken into account, and effective mechanisms must be in place to prevent breaches that would reveal data integrity and confidentiality. This not only involves

preserving the data content itself, but also guards the system guarantees provided to businesses, i.e. business KPIs, and service stability and reliability. The requirement for data confidentiality must be met alongside the legal regulatory requirements for law enforcement access to data (such as Lawful Interception (LI) and Data Retention); if these requirements are assessed early in the design process, then there is the maximum opportunity for meeting both law enforcement requirements and data confidentiality principles simultaneously. Please see NFV-SEC-011 Clause 4 [17], NFV-SEC-009 Clause 4.5 [18] and NFV-SEC-010 [19].

- ***Service and application genuineness***

Systems must ensure that applications and services are genuine, and only contact those end-points that they are supposed to. This mainly involves Industry 4.0 applications, and is related with test, assurance, and maintenance of these applications. Such applications must be safe to use and reliable.

- ***Edge computing and service vulnerability***

Edge computing is designed to reduce the latency of applications and services by making them available to consumers, i.e. users and devices, closer at the edge of the network where user devices attach to networks or at local data centres that are close to RAN. The new 5G architecture now includes distributed user plane function (UPF) nodes across the deployment area, with dedicated ones close to the network edge. This supports multi-access edge computing services closer to user devices, running on dedicated MEC servers.

The traffic from MEC servers to edge UPF machines must be protected to prevent traffic sniffing attacks. Furthermore, the UPF machines must be physically secured so that they cannot be tampered with, which could lead to vulnerabilities for both control and user plane of the mobile network to/from those UPFs.

Edge computing may leave applications vulnerable to some compromises. Edge computing centres may be low-touch environments, with less secure locations, which requires security of such data centres or box units to be assured. Furthermore, MEC application management and provisioning is an added complexity, which requires application provides to have management and monitoring sessions terminating at their MEC application services.

Edge computing services must make sure that MEC applications can only access authorised information, through API security.

Applications and security protocols must also take into account the fact that in some circumstances only limited edge resources (compute, networking, storage) may be available at the network edge. This shapes the policies to be adopted by security mechanisms and could pose a limitation on some heavy procedures.

3.4.2. Users and Internet of Things

5G networks are envisioned to support a variety of new application scenarios and use cases, which require a range of devices to be connected to the mobile infrastructure via different access technologies. This poses a challenge: all devices have their intrinsic security mechanisms, including their systems, hardware, and software. Furthermore, the traffic generated by 5G-connected devices could be vastly different to what conventional user equipment in legacy systems generate. Support for standard security mechanisms may not be readily available at each device, which requires case by case analysis of each device type.

- ***Device genuineness***

Similar to services and applications, it must be ensured that devices are reliable, and trustable. Test and assurance of sensors for factory machinery and automation are critical tasks, and the safety, security, and reliability of devices must be ensured for a fully secure automation system, especially when it is connected to networks. Malware in devices of various types opens up a new security threat surface. Firmware hacks equivalently pose a threat, undermining devices. Some sensors may be extra susceptible to alterations, and open to modifications.

One obvious attack type that affects the system as a whole and damages business KPIs for many users, if not all, is a *distributed denial of service* (DDoS) attack. Networks must have DDoS protection mechanisms against attacks from external sources, which in many cases originate from Internet servers. Coordinated distributed denial of service (DDoS) attacks may occur, generated at rogue or even authenticated devices, and measures must be in place at different parts of the system to identify and mitigate DDoS attacks. TFTP (Trivial File Transfer Protocol) Man in the Middle (MitM) attacks may cause ongoing communications to be overheard by third devices.

Secure storage and processing of user credentials must be ensured by means of tamper-free secure and genuine UE hardware.

- ***User consent and data handling mechanisms***

Besides user privacy and data security mechanisms that have been integrated with mobile communication protocols, further system integration is needed with new building blocks that provide consent and data handling mechanisms. These blocks must be linked with new billing and value chain distribution management systems. Such integration is necessary to build a new secure ecosystem that enables user and business trust in 5G networks and applications. Integration of security systems with data, consent, and billing mechanisms will also help to build an understanding of the risk and liability relationship between stakeholders and risk owners.

- ***Resource limitation of Machine to Machine devices***

M2M devices have significantly lower power consumption and different data transmission patterns as compared to conventional data centre and communications equipment. Security designs in typical mobile networks are provisioned for common

UEs, i.e. mobile phones, laptops, personal digital assistants (PDAs), etc. Protocols also need to be tailored for low-power consuming devices, and not overload them with demanding operations. Hence, security designs must have solutions for M2M use cases, i.e. mIoT in 3GPP, which enables light-weight approaches to conventional security problems, whilst not undermining security operations and not leaving backdoors that could impede system security. Security solutions must also take into account some critical communication applications that involve M2M devices, requiring stringent latency and reliability levels, particularly on the user plane (<4ms RTT). In short, M2M/IoT devices (or gateways for these devices) require security algorithms and procedures to strike the balance between energy efficiency, battery life, and high security assurance.

- ***Identification of M2M/IoT devices***

As 5G networks have an abstract definition of NAS (non-access stratum), identification and authentication of devices will no longer be only SIM-based. This could create new types of security threats to operation and maintenance of networks, particularly for IoT devices which are likely to use flexible identification methods, such as soft-SIM. Hence, identity management procedures should be in place for not only conventional user equipment but also for IoT/M2M devices.

3.4.3. Inter-networking across organisational boundaries

5G networks require connectivity of various network access technologies, different types of adjunct networks supporting new 5G application types, each potentially managed by different operator domains. With the introduction of new players in E2E services, such as virtual infrastructure providers, virtual network service operators, and virtual application vendors, the eco-system in 5G is now more involved than legacy systems.

- ***Operator models***

In a neutral host model, the responsible party for ensuring security must be determined. This spans various network domains, from radio access to the virtual network core. Network hosting in the public cloud, and models such as network as a service (NaaS) introduce new potential security threat surfaces.

- ***Distributed core***

The core network is now being distributed across the network topology in order to reduce user plane latency to devices. Performance-wise this is a highly desired property, yet it also means that it is essential for the core to ensure security mechanisms at its edge networking components which will be away from the main core network data centre. Hence, processes and functions must be in place for device authentication as part of a distributed core management system.

- ***Use of various RAN technologies***

With 5G envisioning many application scenarios, different RAN technologies are getting integrated with 5G, including mmWave, WiFi, LiFi, NB-IoT, and so on. This poses a threat to networks as there are potential risks of such integration when systems are not tested or trialled to detect their unknown/known vulnerabilities. Furthermore, Man in the Middle (MitM) attacks also pose a threat to communication sessions, overhearing ongoing sessions, which may be more likely with different types of access technologies now integrated with 5G networks. Access networks are also vulnerable to jamming attacks, disrupting air interface communications; different access networks operating on different frequency bands all need mechanisms to detect and alleviate such attacks.

- ***Separate ownership of RAN for rural and enterprise use cases***

5G enables many scenarios where separation of interests or separation of ownership occurs between RAN and the core network. The Core must be able to deal with high volumes of moves/changes, i.e. additions/deletions of infrastructure whilst maintaining tight security QoS and control procedures. There might be as many as 1000s of changes per day, affecting macro and micro cells. Furthermore, the networks must be intelligent to detect presence of any rogue nodes, which may be RAN equipment used for malicious purposes. This is more prevalent in 5G networks due to the wide range of access technologies used, the ultra-dense deployment, and various parties that may own different radios.

- ***Backhaul network vulnerabilities***

The backhaul networks connecting sites must be secured by standard IT procedures and security mechanisms, such as DDoS prevention system and security Firewalls towards the public Internet. It is imperative to have mechanisms to detect DDoS attacks within the 5G eco-system, so that devices or rogue RAN equipment do not generate excessive malicious traffic to bring down services servers. Mechanisms must also be in place against IMSI catchers that steal user device identity and pretend to connect to the network but flood communications interfaces.

3.4.4. 5G mobile network and virtualisation systems

To achieve more flexibility and scalability in running network systems and software, and to support dynamic and quick deployment of network services, 5G networks will have integrated NFV solutions, i.e. a virtualised E2E mobile system which is run on virtual infrastructure systems, supporting orchestration and autonomous management of network services. Operators already observe benefits of running virtualisation services in 4G systems, and the roadmap to 5G has emphasised NFV and SDN as supporting technologies. Virtualisation is radically different to legacy mobile systems running on fixed hardware solutions, and has various benefits; nevertheless, it brings about a set of open issues to be addressed for practical deployment in live systems, most of which are related with performance guarantees and security assurance.

The 5GPPP Phase 1 security landscape white paper [20] notes the need for a logical security architecture, which would allow higher flexibility, reducing the criticality of physical allocation of security functions as was the case in legacy systems. This is motivated by virtualisation of services and existence of multiple domains of operation, involving various actors. A logical architecture would allow flexible trust models, security management, and dynamic slicing operations.

- ***Software-based operations***

As opposed to previous generations, 5G networks are more software-based, which poses new threats to operations. For instance, networks must make sure that such software do not get exposed or tampered with, and strong virus protection systems are continuously in operation which are frequently updated and maintained.

- ***Security gaps in networks function virtualisation***

Normative standards on NFV security are underway, and ETSI has draft standards, such as in draft standard GS NFV-SEC-019 [21], building on the report NFV-SEC-12 [22]. However, some substantial and structural security issues may still remain, around isolation of sensitive functions where hypervisors are hostile or compromised.

ETSI also has draft standards on building and testing security monitoring and management for NFV (NFV-IFA-026 [23] and NFV-IFA-033 [24]). These need to be translated into testable solutions (in groups NFV-TST and NFV-SOL) and adopted into open source solutions.

- ***Network slicing***

As stated in Section 1, towards achieving the 5G goals, 5G networks are envisioned to make use of new technologies, i.e. NFV, SDN, MEC, network slicing, and distributed core. This means that any factor that degrades performance of each of these systems is of interest from a security perspective.

5G Networks will be fully virtualised in the mobile core, with multiple network slices running in parallel, dedicated for vertical markets and/or different customer domains. The NFV technology that enables efficient and scalable support for running virtual machines in common-off-the-shelf servers, as well as NFV orchestration technologies, are key to the success of 5G network slices. Operators will benefit from the flexibility and efficiency of deploying virtual mobile core networks in time periods as short as a few minutes, rather than weeks/months.

Core network slices will be associated with matching transport slices with the programmability support provided by the use of SDN in the transport network, i.e. control of SDN switches with protocols like OpenFlow. Furthermore, network slices will support cloud-RAN concepts when RAN sections are dynamically associated with running slices, based on demand and load conditions.

The flexibility and efficiency of network slicing however must be equivalently supported by complete security solutions, which would ensure cross-slice security. This requires the following:

- Full-support for multi-tenancy in an end-to-end network to enable security procedures to have dedicated domains of operations, so as to have complete isolation of slices in the virtualisation systems, It is important to consider the topics from ETSI NFV-SEC-009 [18] and NTV-SEC-012 [22].
- Prevention of unauthorised access between these domains, in terms of authentication methods in place, which would grant access to only authorised users of slices.
- Effective security management and monitoring in virtualised systems (NFV-SEC-13 [25], NFV-IFA-026 [23], and NFV-IFA-033 [24]) will reduce the risk and impact of attacks.
- Resources allocated to a slice are not to be accessible to others.
- Management and monitoring of network slices must be isolated.
- Any potential side channels due to shared virtualisation infrastructure must be prevented (e.g. sequentially used memory locations by multiple virtual machines that belong to different network slices).

When gNB functions are deployed as virtualised network functions (VNFs) on shared virtualisation infrastructure, they may be vulnerable to the attacks typically expected on virtualisation infrastructure. Such infrastructure must be protected against both physical and remote (software based) tampering.

There are new potentially security threats on network slices and the virtualisation infrastructure. Such vulnerabilities stem from the fact that use of network slices in production systems is not wide-spread yet, and its security gaps are still yet to be evaluated fully. Attacks can be on the following:

- Common network interfaces that are shared among network slices,
- Management interfaces to network slices,
- Inter-slice interfaces,
- Slice selection and management.

System restoration after hardware failure

Common issues that are encountered in today's data centres, such as unexpected and unplanned power-down events, pose a risk on continuous and reliable operation of services. There are common practices in data centres to circumvent such situations and bring the system up and restore the system and service context. With the inclusion of NFV-based infrastructures, the orchestration capability provided by MANO systems, and dynamic programmability with SDN, it is now also needed to have NFV, SDN, and MANO to have effective recovery mechanisms in place. Recovery mechanisms in the virtualisation systems must ensure the following:

- The virtualisation infrastructure must be restored completely, with all configurations and settings adjusted correctly. This includes controller nodes pointing to the right set of components, settings reloaded with correct parameters, and full inter-operability restored. Of particular importance is restoring the interoperation between NFV, SDN, and MANO systems, in an automated way, without the need for human intervention to reconfigure these systems to become functional again.
- Services context must be fully restored. This includes reloading virtual machines and network services and setting the last state in place correctly.

Besides virtualisation systems and technologies, 5G networks also have different architectures, which need to be tested not only for its performance but also for potential attack surface it may expose.

Functional split in the new RAN

It is necessary to understand how the new RAN functional splits [26] get deployed, including potential attack paths to limit or deny service layer functions. There might be security implications of splitting RAN protocol stack and distributing them to multiple components. Functional splits in the RAN should address open disaggregated V-RAN. The radio stack now breaks up into separate components as radio unit (RU), distributed unit (DU), and central unit (CU), which may be supplied by different vendors, this may pose a challenge to ensure security and integrity in the RAN system is ensured, considering operations and management of RAN systems.

Multi-level context authentication

Multiple attributes for QoS are now being defined and enabled for context-aware operations in intelligent networks, i.e. various pieces of user context such as applications and usage patterns, and device context such as location and velocity [12]. 5G Networks will benefit greatly from user and device context, so that network slicing operations could be tailored autonomously based on usage demands and patterns. For increased authentication and ongoing security checks and actual delivery of security assurance to users and businesses, there needs to be the ability to efficiently handle and process various pieces of context, and then correlate them with potential security breaches and threats to networks and systems in general. This has the challenge of reducing false positives to a minimum whilst ensuring continuous and secure operations.

Multi-network latency

The 5G networks are more complex than previous generations and includes not only the mobile core network and RAN, but also the transport network, as well as various types of access technologies. This means that there must be effective methods in place to determine, measure and set up deterministic latency levels. Meeting latency targets should not undermine security assurance levels, but it must be also taken into account

that not all application scenarios require the exact same security method; some techniques may be too heavy whereas others may be insufficient. There is certainly a trade-off between performance and security assurance level, as in any other communications system.

- ***Vulnerabilities of previous generations of the 3GPP core network systems***

The new 3GPP architecture for 5G networks [9] supports backward compatibility. This also means that the system will have inherent vulnerabilities from previous generations, i.e. 4G, which must be addressed, especially when a non-stand-alone system is followed.

3.4.5. Physical infrastructure

Beside the software, systems, the users and things, and the services and applications, it is of utmost importance to ensure that physical equipment and system components are not tampered with and are securely installed and can be accessed by authorised personnel only. This not only includes physical access to the infrastructure by human operators, but also access to the systems controlling the infrastructure itself.

- ***NFV and SDN controllers***

The control plane operations related with network slices are performed by NFV functions, and transport layer support is now SDN-based, which decouples routing and switching control operations from the data plane. NFV and SDN provides flexibility, elasticity, and reconfigurability to network operations. However, the use of these technologies also implies vulnerable points in network operations, i.e. the controllers of NFV and SDN systems. It is of utmost importance to ensure that virtualisation controllers are secure and safe and are protected from unauthorised access. This includes the API access to controller services, such as those of virtual infrastructure controllers.

New radio techniques and systems must be tested for not only their performance but also the potential security leaks they may have, and systems, software, and hardware vulnerabilities.

- ***5G new radio***

The new radio in 5G systems is aimed at providing higher data rates than previous generations can do, in the air interface between UEs and the RRH. On the other hand, it is possible that the new air interface technologies, for instance the mmWave technology, now used in some RRHs, is more fragile. This poses reliability issues, which would have side-effects on security.

The use of pico-cells for an ultra-dense deployment as necessary in 5G RAN deployments brings its own challenges. Most notably, air interface attacks may now cover a larger scale with many cells that can potentially be tampered with. This could be in terms of physically obstructing the operation of a cell or tampering with it to interfere or eavesdrop at ongoing communication sessions.

Typical attacks on RAN are denial of service via jamming, especially on control channels, fake base stations (mainly IMSI catchers), traffic interception, mobile device impersonation, location tracking, and network spoofing. 3GPP TS 33.501 [27] has an informative annex (E.1) on UE-assisted network-based detection of false base stations. This mentions that the UE measurement reports have security values that can be used to detect SUPI/5G-GUTI catchers.

- ***Active antenna management***

New active antenna management techniques and similar external actions that manage/configure antenna functionality in real time should not impede or disrupt antenna functions. Such management techniques must be performed by authorised operators or automation engines. Furthermore, transmission beam control towards devices according to control plane information may be vulnerable to intervention/breaches.

Besides the risks involving the new radio and the virtualisation controllers, there are threats to standard hardware equipment and systems that data centres and equipment locations must always address.

- ***Commodity hardware vulnerabilities***

Similar to any system, physical hardware equipment has vulnerabilities that need to be considered. At times of system failure or meltdown it is important to have the system be restored, and in doing so, to reload any security systems to be fully functional once again.

- ***Hardware performance deterioration***

Traditionally IT network hardware may introduce latency issues. e.g. slow firewalls. This poses a risk to meeting customer SLAs whilst protecting the network, users, and services from attacks from outside the system domain.

- ***Physical security of base stations, computing systems, and core networks***

As with any system, this aspect is related with the physical security of these sites, including ease of access to any of the above functions through proximity to physical components, systems, and sub-systems. The challenge in 5G networks is the distributed nature of these systems with potentially many data centres running the core network components, and systems to support MEC operations. Furthermore, 5G networks have dense deployment of RAN equipment, hence more base stations per square km.

3.4.6. Security Layers Summary

The large attack-surface of 5G networks and systems has different vulnerabilities across the five security layers identified in this paper. To ensure a 5G network that not only meets the ITU performance requirements but also prevents the security risks associated with these vulnerability points, companies and organisations from different industry verticals must cooperate through the standardisation bodies and industry forums.

The various verticals in 5G, as illustrated in Figure 7 below, require support from different standards developing organisations (SDO) to define security specifications. Industry focused areas, such as robotics and automation, emergency and critical communications applications and systems on autonomous vehicles and remote healthcare, and user and community focused new technologies, such as augmented reality (AR), virtual reality (VR), mixed reality (MR), all have distinct and challenging security requirements, besides their performance requires as outlined in Section 1. These applications will require a more secure network than legacy systems, which is an added complexity.

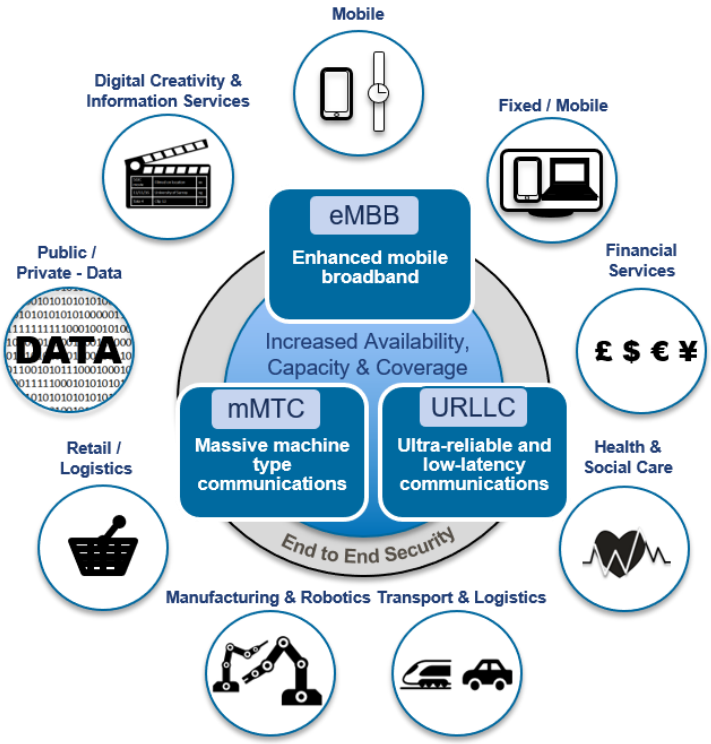

Figure 7. Industry verticals in 5G use cases.

An E2E cross-layer approach that also adopts the security-by-design principle is fundamental to bring all SDOs together and align specifications, so that security in different parts of the 5G system (i.e. mobile core, transport, access technologies, devices, and services and applications) are interoperable. This is necessary to make sure that security solutions offered by a single SDO are not overly-specific with limited scope, leaving security gaps when all parts need to interconnect. Section 4.3 lists the SDOs and industry forums that need to work together on the

security of different parts of the 5G eco-system. A good example of such practise is 5GAA working with 3GPP on transport use cases and standards.

3.5 Security Section Concluding Remarks

Besides the components of the new 5G architecture as defined by 3GPP in the technical specification document TS 23.501 [9], 5G networks have the unique property of merging different types of networks and technologies under one umbrella system, requiring inter-operability, efficiency, and seamless connectivity, and support for the requirements of a large number of diverse use cases. This is indeed a challenging goal, as this complex system of multiple inter-connected networks must also be secured, and not with fragmented security solutions but following an E2E, cross-domain, and cross-layer approach. 3GPP has also defined the security architecture for 5G systems in the technical specification document TS 33.501 [27]. This is targeted at making 5G more secure than legacy systems.

The Collaborators focus on not only systems integration but also security integration with systems and research and development for 5G communications and services. Most deployment testbeds do not have a particular focus on 5G security. Hence the testbeds deployed by the Collaborators are one of the first in which understanding security challenges is one of the pillars for future systems integration, and tests and trials work.

There are several conclusions that can be drawn based on the analysis performed by the Collaborators so far on 5G systems and their security. This paper is aimed to set the initial baselines for security implementation and tests for 5G networks, not only for the testbeds that are being built by the Collaborators, but for similar networks, trials and test beds around the world targeting 5G system(s) integration.

- **Risk appetites and trade-offs – security, system performance and costs**

Due to a number of diverse yet demanding applications and use cases, any additional security mechanism that is built on top of the fundamental ones would address the specific needs of different use cases, which are highly likely to be contradictory, with different stakeholders and risk owners involved. Hence, effective security mechanisms in 5G networks should be defined from the perspective of different user groups and also from the risk appetite of the network operators in providing services to all or some of these user groups. There is also an inevitable trade-off between multiple variables related to cost, security and performance. This must be taken into account when activating security mechanisms, so that promised service level agreements can be provided to costumers. Tolerable levels in the network performance, such as data download/upload rates or latency, should be determined to better evaluate the trade-offs in place. It must be noted that not all 5G user cases and services will require the same level of security, hence there must be requirements for security levels and mechanisms that must be in place for each use case, and recommendations on necessary minimal security settings must be designed and tested. Requirements should be captured to help decision making processes for both the 3GPP Release 16 standards and the 5G live UK national roll-out.

- **Security by Design**

The approach taken by the Collaborators is 'Security by Design' where practically possible and/or available, which means considering security at the earliest stages of system development, i.e. at pre-design concept phase or critical design decision points. This requires security mechanisms to be embedded with communication protocols, infrastructure systems, covering all aspects of an E2E communication system. By reflecting user risk requirements and incorporating key security principles at key decision points, users and operators will have a better chance of meeting some of the security challenges posed by 5G. Operators can then enable additional security mechanisms when necessary, on a per-use case basis.

A new or existing organisation that is tasked or formed to help monitor and encourage good security-by-design practice is needed and highly recommended. This organisation would set out and document an approach to designing secure 5G networks, applications and services that will be required to deliver critical services, operating across multiple organisational boundaries.

- **Security trials and tests for risk assessment**

Risk assessments against a set of criteria/principles must be performed ahead of the roll-out of key 5G milestones, such as a 3GPP Release 16 compliant system. This will help determine next steps and strategies for each risk factor. Based on the findings from trials and tests, advice for businesses and operators investing in DevOps or application development on how to approach risk decisions could follow, further improving system security. Furthermore, by providing advice, operators and administrators would be providing a description of the lowest-bar of entry on the network. This would not only assist operators in ensuring some basic security controls are in place but also aid 5G network monitoring for 'non-conformist' or 'mischievous' deployed software.

- **Context-aware networking and artificial intelligence**

The dynamicity in 5G networks, in terms of user mobility, application use and data rate requirements, as well as variations in network conditions require autonomous operations that improve performance of the 5G services provided to all users of 5G. This calls for effective mechanisms to continuously monitor network state at various points of operation at component systems. Input from monitoring agents are then to be used by automation engines to derive artificial intelligence decisions to predict patterns. Such patterns can then be used by decision making engines that empower an intelligent 5G core network that can lead to effective use of network slices and system resources. They would also help traffic engineering algorithms to better use network resources in the transport network.

Artificial Intelligence (AI) driven operations will use location awareness, user and device context handling and processing, as well as dynamic association of device and user relationships.
AI can help networks to be significantly more efficient and secure. However, poorly defined AI systems and algorithms themselves could increase the potential attack surface and expose further security vulnerabilities.

Besides communication systems operations, security assurance can also benefit from context-aware networks. Security mechanisms will make use of not only current collected security context from the network but also predicted future changes security patterns acquired by predictive operations that can track security patterns and identify potential vulnerabilities in

real time. On the other hand, user context acquisition and processing must not prejudice user privacy.

- **Network visualisation**

Visualisation of the 5G networks is central to actively monitor network state, especially in the complex environment running various types of services and due to existence of virtualisation systems, i.e. NFV, SDN, and orchestration of network slices. It is also necessary for monitoring any potential vulnerabilities, which also require active alarm triggering mechanisms.

- **Cooperation for security standardisation**

To achieve an E2E cross-domain cross-layer security in 5G systems, industry and SDOs must cooperate to design and define necessary mechanisms, their interfaces, and inter-operability. The efforts must focus on not only security in networking and communications but also applications.

4 Appendices

Further information on 3GPP 5G security standards, the testbeds of the DCMS 5G T&T programme and a list of standards developing organisation (SDO) and industry forums can be found in the following appendix section. First, 3GPP security for 5G are presented. Then, details on the testbed projects of the Collaborators are provided. Finally, the SDOs, industry forums and alliances, and several EU 5G PPP projects working on 5G networks and security are listed.

4.1 3GPP security for 5G networks

The 3GPP SA3 Group have defined the security architecture of 5G mobile networks in specification document TS 33.501 [27]. This document outlines security domain definitions, and also points to some security features in 5G systems. In the following section, essentials on 5G mobile network security introduced by 3GPP are summarised. Where applicable, the improvements of security from legacy 4G networks are also listed.

4.1.1. From 4G to 5G

Compared to 4G networks, which have IPsec tunnels between protocol components to assure network domain security, 5G networks have transport layer security (TLS) [28][29] and application layer security in place as well, based on the service-based architecture (SBA). All network functions shall support TLS with client and server side certificates. TLS will ensure transport security within an operator domain. NDS/IP may be used to provide Network Domain Security (NDS) [28][30]. The use of cryptographic protection in NDS is left to the operator decision and depends on whether component interfaces have been physically secured in trusted locations.

When the 5G core is implemented based on SBA, 5G network functions are designed to be modular, with interfaces to be implemented according to SBA principles. According to this

approach, all northbound Application Programming Interfaces (API) are to be protected by Common API Framework (CAPIF) [32], making it possible to have a single protection scheme used for all system functions. In comparison, protection of the northbound APIs of protocol components is fragmented in 4G.

5G networks will have further improvements as opposed to 4G networks:

- 5G introduces certificates for IoT devices, in additional to the 5G-AKA security mechanisms.
- 5G enables integrity protection for user plane traffic. Security of the user plane is either disabled or enabled for all dedicated radio bearers in 4G, whereas 5G enables selective protection per PDU session. It must be noted that this feature will require more resources at both the gNB and the UPF (core network user plane function).
- In 4G, device IMSI is not protected if there is no security context in place. In contrast, SUPI is protected with asymmetric cryptography in 5G.
- The home control feature in 5G security enables the network to verify device location when the device actually is in a visited network. This step has been taken to prevent spoofing attacks on device locations. This is a vulnerability in 4G networks, which involves false signalling messages to request device identifier and location, and then intercept ongoing communications.
- 5G security includes the concept of “unified authentication”, which means 3GPP (5G RAN) and non-3GPP access networks (e.g. WiFi) need to employ the same authentication methods. The authentication procedure over 3GPP access can provide keys to establish security in untrusted non-3GPP access. The UE and the networks will support both EAP-AKA’ [31] and 5G AKA authentication, regardless of the access network type. This will be possible for only new WiFi equipment which support use of foreign keys from 3GPP networks.
- 5G has a mitigation method against bidding down attacks. It prevents a fake base station from making UEs believe that the base station does not support a specific security feature and hence force to use a previous mobile network technology. Such base stations are referred to as *IMSI catchers*. In 5G, the whole coded and protected NAS messages would need to be captured to mimic a base station; hence it is harder in 5G for IMSI catchers to succeed.
- 5G UE and the home network can set which mobile technologies can be used, i.e. 4G, EDGE, 5G, etc. Such settings will be remembered and restored after device power off. Only emergency services can override this selection and are allowed to use any technology supported by the device which is available.

The specification document TS 33.501 [27] lists many more definitions and features, some of which are presented in the following sections.

4.1.2. Security domains

The 3GPP security architecture includes a number of security domains in an E2E 5G mobile system, as illustrated in Figure 8.

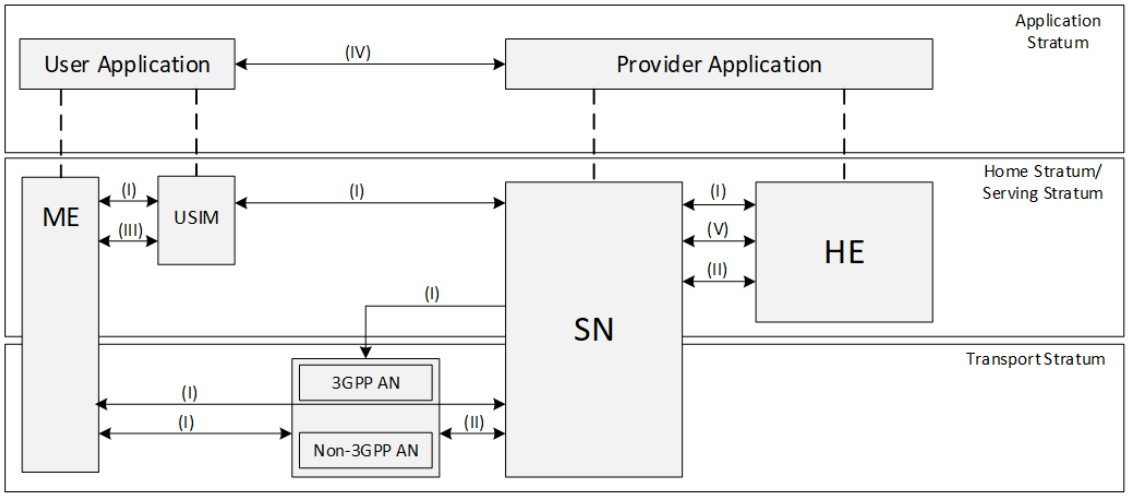

Figure 8. Overview of the 3GPP 5G security architecture [27]. SN: Serving Network, HE: Home Environment, AN: Access Network, ME: Mobile Equipment, USIM: Universal Subscriber Identity Module.

These security domains are:

- Network access security: Includes UE authentication and access to the mobile network. It focuses on 3GPP and non-3GPP (e.g. WiFi) access, and in particular to protect against attacks on radio interfaces. It also involves security context delivery to the access network (See interfaces I in Figure 8).
- Network Domain Security (NDS): Ensures that network nodes can securely exchange signalling and user plane data. (See interfaces II in Figure 8).
- User domain security: Includes the security features that secure user access to mobile equipment. (See interfaces III in Figure 8).
- Application domain security: Includes the procedures to ensure that applications in the user domain and the provider domain can exchange messages securely. (See interfaces IV in Figure 8).
- Service based architecture domain security: Includes features to ensure network functions can securely communicate within the mobile network and with other network domains. (See interfaces V in Figure 8).
- Visibility and configurability of security: Includes the set of features that enable the user to be informed of the availability of a security feature (not presented in Figure 8).

4.1.3. Security entities in the 5G core network

Control plane security and confidentiality between UE and the network core is ensured by a number of network functions. The SEcurity Anchor Function (SEAF) in AMF of the 5G mobile core, as well as the AUthentication Server Function (AUSF), the Subscriber Identifier De-concealment Function (SIDF) and the Authentication credential Repository and Processing

Function (ARPF) at UDM play the central role in 5G system UE authentication procedures. AMF also includes functionality to store security context by means of a Security Context Management Function (SCMF) [33].

4.1.4. Authentication and Authorization

In 5G, the primary protection of UE traffic is assured between the UE and the AMF in the 5G core. A secondary protection based on Extensible Authentication Protocol (EAP) [34] is established between the UE and the AAA server in external data networks, where the core network element SMF plays the role of an authenticator[5]. This secondary protection is optional, but is encouraged for the user plane.

AMF triggers primary authentication of the UE using the Subscription Concealed Identifier (SUCI), which is a one-time temporary user identifier. It then assigns a 5G-GUTI to the UE and supports reallocating the 5G-GUTI to the UE when necessary, i.e. when roaming takes place. This is performed on both 3GPP and non-3GPP access. The security anchor function (SEAF) is the function at AMF that performs primary authentication procedures and stores the security profile on a per subscriber basis for the duration of their registration.

Subscription Permanent Identifier (SUPI) is used for UE authentication and key agreement. SUPI is not to be transferred in clear text form over 5G-RAN.

Authentication keys will bound to the serving network, which is a step against network spoofing. This is called serving network authentication and covers access networks for 5G networks and non-3GPP authenticated access, such as Wi-Fi nodes.

4.1.5. Data confidentiality and integrity

5G Core and 5G RAN shall enable encryption and integrity protection algorithms.

Integrity protection and replay protection for user data are mandatory to be supported at UE and gNB, but their use is optional. Integrity protection of user data adds overhead on packet sizes and increases processing load at gNB and the UE. However, operators are urged to activate integrity protection for user data. As for NAS and Radio Resource Control (RRC) signalling, integrity protection is mandatory.

Confidentiality protection of user data, RRC signalling, NAS signalling are optional. Operators are urged to implement and enable confidentiality protection mechanisms, whenever regulations permit.

Configuration and setup of gNBs by the OAM systems shall be authenticated and authorised by gNB. The communications between gNBs and OAMs is protected for confidentiality, integrity, and replay. Certificate enrolment mechanisms are specified, but their use is left to operators.

gNB interfaces between the CU and the DUs, i.e. F1 and E1, must ensure and support confidentiality, integrity, and replay protection. This includes management and user plane traffic.

[5] SMF relies on the AAA server to authenticate and authorise UE's request for PDU session establishment. SMF communicates with the AAA server over the N4 interface, where UPF relays the messages between the AAA server and SMF. EAP message communication between the SMF and the UE is through the AMF.

4.1.6. Subscriber privacy, and secure storage of credentials

Tamper resistant secure UE hardware shall ensure integrity protection for subscription credentials. Authentication algorithms shall be executed within the tamper resistant secure UE. Permanent Equipment Identifier (PEI) (IMEI in legacy 4G networks[6]), which uniquely identifies the user equipment, is only transferred after security context has been established.

Any part of the gNB that stores and processes keys and control or user plane traffic in clear text must be protected from physical attacks. gNBs should be located at physically secure environment, which supports secure storage of sensitive data (cryptographic keys and configuration data), execution of sensitive functions (encryption/decryption, authentication), and execution of boot processes.

Subscriber privacy enablement is under the control of the operator. Subscribers are assigned with a globally unique Subscription Permanent Identifier (SUPI), which includes UE IMSI as well as home network identifiers. SUPI is not disclosed during connection establishment. Instead, the Subscription Concealed Identifier (SUCI) is exchanged, which is generated by the UE. Fake base stations (IMSI catchers) cannot identify the subscriber identity, as SUPI is only revealed after full connection establishment, involving the core network. The Subscriber Identifier De-concealing Function (SIDF) at the UDM, which only accepts requests from network functions of the home network, de-conceals the SUPI from the SUCI.

4.1.7. Inter-domain operations in 4G and 5G systems

There is an open issue in 4G mobile networks concerning the inter-domain operations between two network operators through Internetwork Packet eXchange (IPX) networks, which allows user information to be revealed across IPX networks.

To address this issue, the service-based architecture of 5G mobile networks include a security edge protection proxy (SEPP) entity, interfacing with IPX networks, and hence confidentiality and integrity is at the edge of the network between network operator domains. SEPP implements application layer security for all the service layer information exchanged between two NFs across operator domains. This prevents IPX providers from reading sensitive information, such as authentication vectors. Note that, for the mobile core interfaces within an operator's domain, there is no need for such a proxy, but transport layer security is still needed between core network functions[7].

SEPP can also detect any unauthorised message modifications. Authorised changed include those made to parameters necessary for interoperability. It also performs message source validation, message format verification, and topology hiding.

In additional to transport layer security, application layer security is also needed between network functions so as to protect information elements exchanged between network functions of different operators.

[6] For non-3GPP access in 5G, Wi-Fi station ID could be PEI.

[7] CAPIF security protects northbound APIs of core network functions in 5G SBA.

4.1.8. Security context in the 5G core

Establishing security mechanisms is part of mobile connectivity and session establishment procedures. Repeated security set-up processes may slow down initiation operations, which adversely affects user experience. If fresh authentication procedures could be avoided as much as possible, this would help to reach 5G application QoS requirements. This is possible by means of keeping a security context in the core network and enabling reload of security context when possible. The new 5G core networks can then seamlessly preserve user confidentiality and privacy without sacrificing performance, whilst ensuring that security settings are maintained and managed efficiently. For instance, inter-system handover (or idle-mode mobility) between the 5G core and legacy 4G core networks can be performed without re-establishment of entire security context of devices.

The SEAF provides the capability to re-authenticate a mobile device without the need for full authentication methods, e.g. key agreement procedures. AUSF can produce anchor keys that can be used to generate keys to be used in more than one security context. The SEAF is expected to also manage the security context for each subscriber that is Registered at this AMF, in a management function, such as a Security Context Management Function (SCMF) [33].

4.1.9. Artificial intelligence to support context-aware mobile core and network security

One supporting technology in a context-aware mobile core network is artificial intelligence (AI) which can process context transfer patterns and correlate them with user, device, application, and security context meta-data to make predictive decisions. This will assist mobile core network operations as it would make sure the network set up is one step ahead of the dynamics in user behaviour and context.

4.1.10. Security gateways

Security gateways (SEG) are entities to be used on the borders of IP security domains to secure native IP based protocols. The number of SEGs to be used in a security domain depends on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and to avoid single points of failure [35].

In the 5G system architecture, the N2 interface between RAN and AMF may use a security gateway at the AMF side as terminating point. IPSec Encapsulating Security Payload (ESP), Datagram Transport Layer Security (DTLS), and IKE-v2 security certificate-based authentication are to be used between RAN and the core, both on control and user planes. Integrity, confidentiality, and replay-protection are the essentials. The use of cryptographic solutions is left to operator's choice [28][30].

Within the RAN, between the gNB central unit (gNB-CU) and gNB distributed units (gNB-DUs), IPSec ESP and IKE-v2 security are to be used. A security gateway may be used at the gNB-CU side. DTLS is also to be used for integrity, confidentiality, and replay protection. It must be noted that deployment of such security solutions between gNB-CU and gNB-DU must not cause time

alignment and synchronisation issues over control and user planes. The use of cryptographic solutions is left to operator's choice.

For non-SBA internal core network interfaces, such as N4 and N9, NDS/IP is to be used to ensure integrity and confidentiality protection.

4.1.11. Network Exposure Function

Network functions (NFs) in 5G expose their capabilities and events to a network exposure function (NEF). Third party application functions (AFs), which reside outside the 5G mobile core, can retrieve NF capabilities and events via the NEF. This is performed securely via TLS client-server certificates. Application functions must be authenticated and authorised by NEF using an OAuth-based [37] authorisation mechanism. NEF may support CAPIF [32] as well.

4.2 Testbeds of the DCMS 5G T&T Programme

As part of the DCMS Phase 1 5G T&T programme [1], three testbeds are being built: Worcestershire, 5G RuralFirst, and AutoAir. In addition to these new testbeds, 5G Innovation Centre (5GIC) provides its virtual 5G core and radio network, making it a nation-wide 5G testbed eco-system. In the following section, the three DCMS Phase 1 project testbeds and the 5GIC testbed are explained.

4.2.1. AutoAir, Millbrook

4.2.1.1. Scope and expected impact

The AutoAir project is a neutral host solution based on 5G small cells for transportation networks in the UK. This type of 5G network enables a range of service providers and end users to access shared 5G network capabilities, i.e. eMBB, mMTC and URLLC and will also accelerate the development and deployment of CAVs.

The testbed will be a reference Hyper-Dense 5G network for urban centres and for the UK's transportation corridors, enabling industry from many sectors to understand and test their applications with 5G.

The Millbrook testbed will be offered as a service to the auto Industry, Network Operators and other sectors wishing to test a shared 5G network. The testbed will make the UK a world leader in 5G, transport use cases and CAVs and help to reduce the time to market for the project partners.

4.2.1.2. Industry involvement

AutoAir consists of a partnership including leading 5G players and auto industry leaders, who can immediately make use of the testbed to accelerate the development of CAVs and test the benefits of eMBB, mMTC and URLLC. This partnership includes 5GIC at Surrey University, Dense

Air Ltd, McLaren Applied Technologies, Blu Wireless Technology Ltd, Quortus Ltd, Millbrook, Real Wireless, ARM, Cobham Wireless, and Celestia Technologies.

4.2.1.3. Infrastructure and architecture

AutoAir project will see Millbrook, the location near Bedford where proving ground for this testbed is, build a fibre backbone and 59 small cell base station sites. This 5G small cell infrastructure consists of both access and backhaul solutions, combined with a 5G Non-Standalone core network. The testbed is split into multiple functional areas as shown in the following system architecture diagram, in Figure 9.

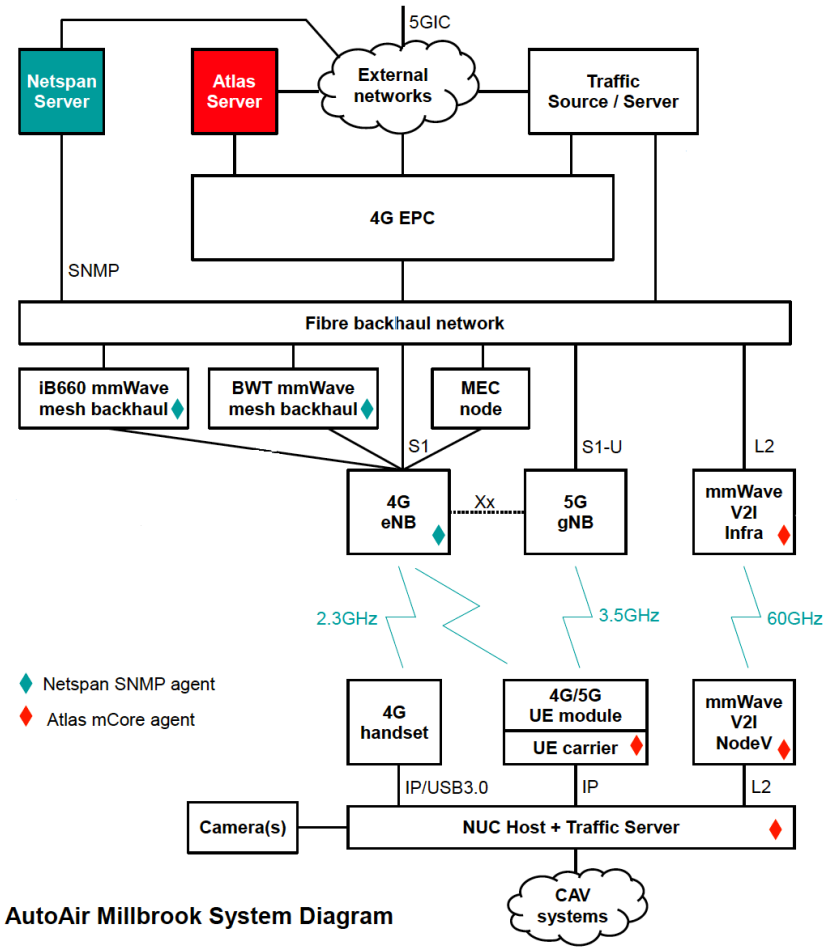

Figure 9. AutoAir Millbrook System Architecture.

The "AutoAir" testbed consists of two locations, used for different purposes. The first is at 5GIC at University of Surrey and the second location is at Millbrook. The testbed will be operational by January 2019 and will be jointly operated by the network operator Dense Air, 5GIC and Millbrook.

The architecture is logically split into Core and Edge (MEC) network with OAM capabilities and a series of V2I CAV functionality. The architecture also offers eNB splitting through S1 splitter to allow different operators access to different slices of the network.

The implementation of Edge network (MEC) functionality is achieved through the separation of Control and User Plane (CUPS).

4.2.2. Worcestershire

4.2.2.1. Scope and expected impact

The Worcestershire testbed comprises of 4G and 5G RAN deployment on its five partner sites, connected to the 5G core network hosted at 5GIC. The testbed offers an E2E 5G system for tests and performance measurements. It also hosts MEC services at two of its partner sites. The deployment architecture supports E2E network slicing from RAN to the core network, where each partner site can be allocated with a network slice for the use cases enabled by the site.

4.2.2.2. Industry involvement

Several partner sites make up the Worcestershire testbed. These are 5GIC, Malvern Hills Science Park (MHSP), Yamazaki Mazak, Worcestershire Bosch, QinetiQ, and Heart of Worcestershire College. These partners are involved in use case and scenarios for 5G, tests of the system, and later making the system available to 5G users. BT, AWTG, Telefonica and Huawei are collaboration partners supporting the testbed deployment.

4.2.2.3. Infrastructure and architecture

Several RAN networks have been deployed in the Worcestershire testbed to enable 4G and 5G RAN connectivity. This deployment follows availability of hardware and systems in 5G RAN technologies, and is performed in stages of upgrade, starting from off-the-shelf LTE solutions, later migrating to 3GPP Non-Standalone Architecture (NSA) option 3.X. NSA allows for co-existence of 4G and 5G RAN equipment and their connectivity to the 5G core (5GC), where the 5G NR supports data plane whereas the LTE RAN carries the control plane traffic flows. 4G eNB and 5G NR have an interface to exchange control plane messages over the X2 interface.

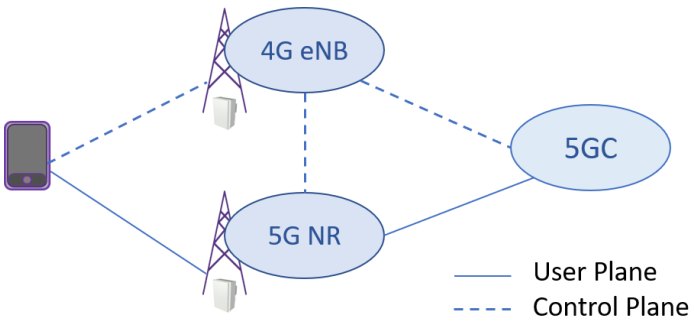

Figure 10. 3GPP NSA option 3.X - 5G eNB and 5G NR deployment in the Worcestershire testbed[8].

The 4G and 5G RAN comprise of both indoor and outdoor deployments. The remote radio head (RRH) units are accompanied by varying numbers of base-band units (BBU) to fit the requirements for the partners' communication needs.

[8] The deployed architecture is a pre-standardised version of 3GPP NSA Option 3.X.

5G Core provides distributed 5G network functionalities operating at the network edge on secure MEC nodes. The MEC servers also provide capability to run service and applications at the network edge.

Security testing of the infrastructure will comprise of multiple information assurance testing techniques, ranging from policies and controls to technical and architectural configurations. Penetration and radio frequency testing will also be used as part of a suite of tools.

The Worcestershire testbed supports 5G NR deployment on selected partner sites, all connected to the 5G virtual core network running at the 5GIC testbed.

In its first stage of deployment, the partner sites in Worcestershire are inter-connected through a non-SDN switch, for the purpose of E2E tests and system functionality validation. This inter-connection also links the Worcestershire testbed to the 5G Core and the Internet through the 5GIC testbed. In Q1 2019, the second stage of deployment will inter-connect the partner sites at this aggregation point via an SDN switch, as illustrated in Figure 11.

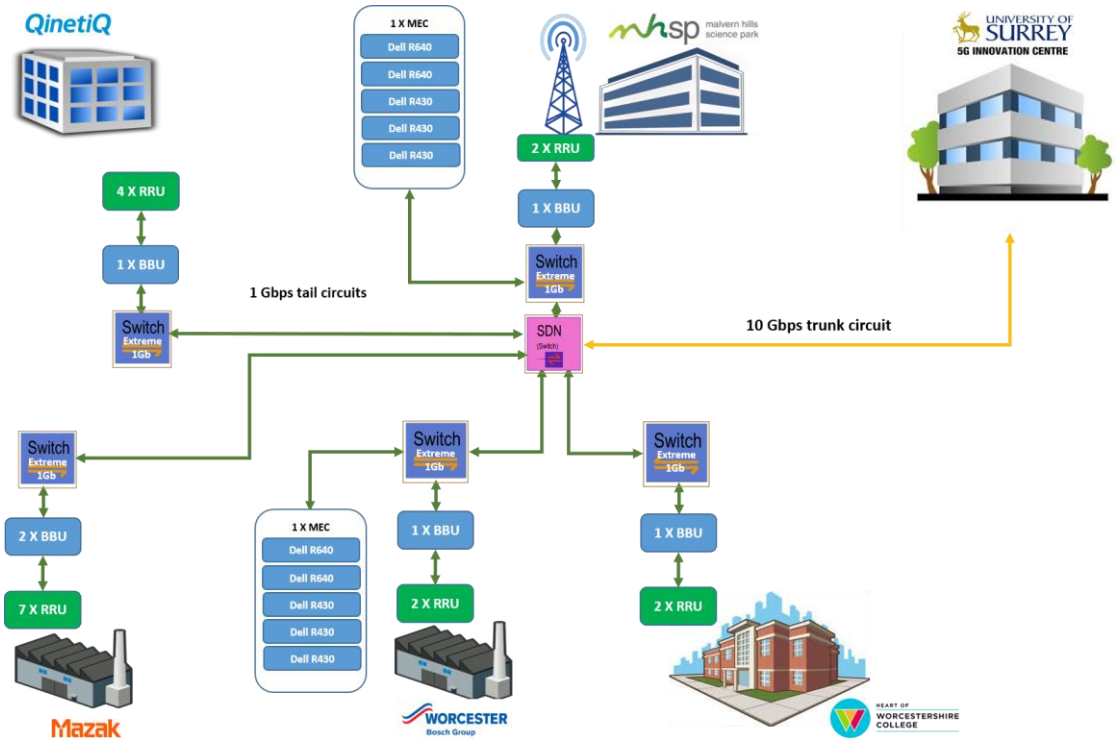

Figure 11. Logical architecture of the Worcestershire 5G testbed. The SDN integration point is hosted at the MHSP partner site.

4.2.3. 5G RuralFirst

4.2.3.1. Scope and expected impact

5G RuralFirst (5GRF) is built as a complete end-to-end 5G testbed system for trials of new 5G wireless and network technologies, wireless services to rural communities, spectrum sharing, new applications and services, and new business models. The system has a focus on testing and demonstrating innovative approaches for ensuring that 5G connectivity is accessible and

affordable in hard-to-reach rural areas. The testbed includes radio access networks in three locations: Orkney, the Hands-Free Hectare in Shropshire, and Beard Hill Farm in Somerset.

The testbeds and trials implemented and demonstrated by 5G RuralFirst are firmly based on some use cases which represent genuine challenges faced by rural communities and industries. These communities strive to develop viable ways of ensuring that they are 'digitally connected' and well-positioned to keep up with the various benefits and opportunities to be generated by 5G. This is especially of significance in today's world of increasing reliance by businesses and individuals on the use of on-line services and applications.

5G needs to be more than simply 'better 4G', otherwise rural communities would remain poorly connected. In particular, opportunities exist for the development of a 5G eco-system that goes beyond being purely 'mobile operator'-centric, and instead embraces new approaches to enabling rural communities and alternative communications providers to deploy 5G services in areas where traditional Mobile Network Operators (MNOs) are not operating, or, where appropriate, to provide enhanced services that complement those being provided by MNOs. To this end, the use cases are concerned with more than simply the use of new radio access technologies; they extend to new ways of managing and accessing radio spectrum, new business models, and the combining of new 5G technologies with legacy technologies to achieve cost-effective mobile and fixed connectivity in hard-to-reach rural areas. Affordable infrastructure and access to spectrum are key enablers in this regard, both of which form key 'themes' in the project.

The use cases being deployed within 5G RuralFirst project can be summarised as follows:

- **Orkney**
- *Community Mobile Broadband*: Test of different technologies, including lower cost solutions, to deliver connectivity to several communities, where nothing, or only very poor landline coverage exists today.
- *Optimised Tourism*: Despite having only 20,000 inhabitants, the Orkney Islands received over 110,000 tourist visitors last year. Through deploying connectivity to tour buses, 5GRF will enable passengers to access dynamic content, helping to manage tourist density during peak times, and an enhanced passenger experience.
- *Broadcast 5G*: Test of the potential of 5G to broadcast nationwide in a more efficient manner. The broadcaster BBC can only turn off terrestrial TV when alternatives can cover 99% of the population. Hence, diverting broadcast costs to 5G mobile network operators could be a valuable contributor to the 5G rural business case.
- *Ferry Connect*: 26GHz/mmWave backhaul connectivity for a ferry operating between two of the Orkney Islands, which will fill a gap at one end of the journey where the ship loses WiFi connectivity from the main port.
- *LiFi*: Testing of the viability of LiFi (Infra-red) in harsh rural environments, by connecting a number of rural properties using solar panels as receivers.
- *Legionella Detection*: IoT-enabled remote monitoring of water in a local school will provide a cost-effective solution for health & safety compliance.
- *Aquaculture Health Monitoring*: Farmed salmon is the UK's second largest food export, and therefore a major contributor to our national economy. Measuring

parameters (pH / dissolved oxygen / salinity / temperature) inside and outside the salmon cages is vital, as exceeded parameters can pose a serious risk of death to the fish stocks. It is essential to continuously monitor the farms remotely and ensure optimal operating conditions. Despite this being a tech heavy industry, deployment today is seriously constrained by limited connectivity.

- *Connected Wind Farm:* IoT sensors will enable high value equipment integrity monitoring as well as weather/wind speed monitoring. Installing this tech could help identify potentially dangerous weather conditions, and enable appropriate action to be taken, minimising impact. This in turn could reduce insurance premiums, helping to improve the efficiency of wind farms.

- **Hands-Free Hectare (HFH), Shropshire and Beard Hill Farm, Somerset**
- *Autonomous Tractors:* This use case will explore the value of autonomous tractors, controlled by drones in real time via 5G connections.
- *Drone Soil Analysis:* Drone analysis and tractor control to spray fertilizer on needed areas.
- *Virtual Vets:* An Augmented Reality (AR) use case, offering remote veterinarian diagnostics support, enabling farmers to ask advice and see how to care for animals in real time, using voice commands.
- *Connected Cows:* Test of the ability to proactively manage animal health, through monitoring of rumination, fertility, and eating patterns.
- *Weed Detection & Treatment:* Drone footage will be analysed using machine learning algorithms to identify weeds and how to treat the soil in real time using 5G.
- *Hyperspectral Imaging:* Real-time identification and classification of soil conditions from a plane flying at 900 metres, to enable more rapid, real time response to soil conditions, cattle grazing patterns, and spread of disease in forests.

4.2.3.2. Industry Involvement

The project consortium of 5GRF is formed of a larger number organisations from industry and academia, including network operators, service providers, companies for backbone connectivity or radio access technologies, research centres, and universities.

4.2.3.3. *Infrastructure and Architecture*

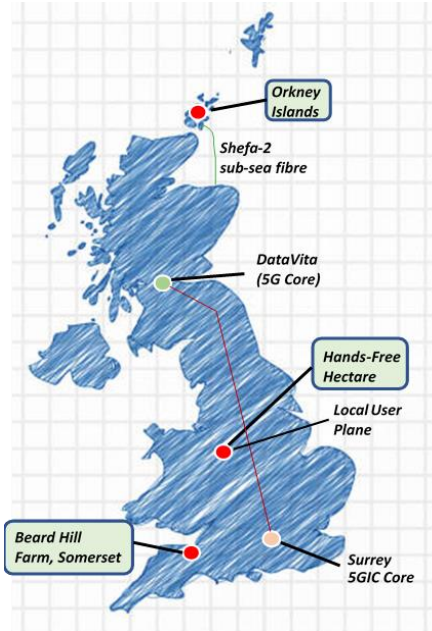

Figure 12. 5G RuralFirst network deployment locations in the UK.

Figure 12 illustrates a high-level diagram of the 5G RuralFirst network. The three testbed locations (Orkney, Hands-Free Hectare, and Beard Hill Farm) are connected by various means to Cisco's 5G virtual core and cloud services at its DataVita data centre, which is a Tier III data centre situated roughly halfway between Glasgow and Edinburgh.

- **The backbone:** 5G RuralFirst's core network comprises a number of high-capacity links which connect the testbed locations to the virtual core and cloud services at DataVita. Orkney is connected to the UK mainland via Shefa's sub-sea optical fibre cable, while connections on the mainland are formed from leased connections provided by Abica.
- **The core network:** The virtual core is being implemented at DataVita data centre. The radio access networks (RANs) at each of the three testbed locations (Orkney, Beard Hill Farm, Hands-Free Hectare) connect to the core at DataVita, where orchestration and network slicing are implemented.

The project will also explore cost-effective infrastructure sharing models including neutral hosting and not-spot roaming; these will make use of 5GIC's virtual mobile core network in addition to the virtual mobile core at DataVita.

In one particular use case at the Hands-Free Hectare, Shropshire, (Figure 12) there are stringent latency requirements which necessitate the deployment of a local user plane function (UPF) at that location.

4.2.4. 5G Innovation Centre (5GIC)

4.2.4.1. *Scope and expected impact*

The 5G core network is based on the Flat Distributed Cloud (FDC) architecture [12] with dynamic slicing as shown in Figure 13 below, and is an evolution from the 4G+ context-aware core also available at the 5GIC [14], which is designed according to 3GPP system architecture components [9].

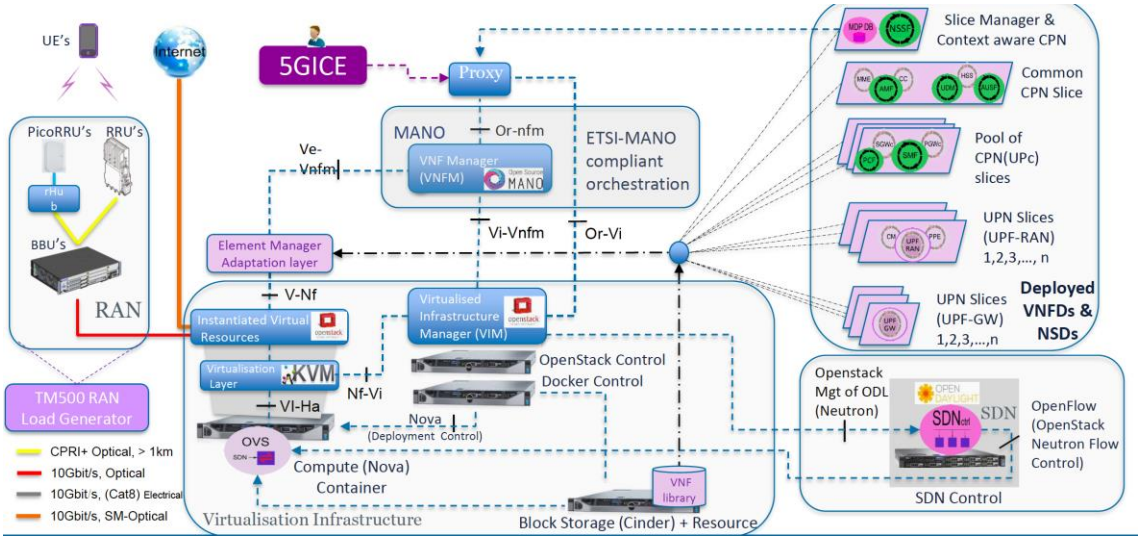

Figure 13. 5GIC Virtualisation system architecture.

4.2.4.2. Industry involvement

The 5GIC testbed development and deployment is overseen and supported by 5GIC industry consortium [36], which includes network operators, providers, vendors, a large group of SMEs, and content providers, as well as UK academic institutions. The Centre has been developing cutting edge mobile network technologies and demonstrating these systems and technologies in regularly held workshop events.

The testbed is designed and developed to support next generation of mobile network technologies, particularly virtual and orchestrated core network deployment. Proof of concept and full E2E mobile network services are supported by the testbed infrastructure, creating an ideal research and development environment for researchers and SMEs.

4.2.4.3. Infrastructure and architecture

The 5GIC testbed has various features that make it an ideal research and innovation platform for 5G networks.

- **Open source deployment**

The virtualisation system as illustrated in the figure is based on open-source software components, i.e. OpenStack [38] as NFV infrastructure controller, OSM [39] as its ETSI NFV MANO [40] orchestrator, and OpenDaylight [41] and Ryu [42] as the SDN controllers. The virtualisation system runs multiple core network slices, each associated with a different 3GPP use case, or allocated to each user of the system. The system has been designed to support orchestrated deployment of these network slices.

- **Middleware to deploy network services across testbeds**

The testbed also has an integrated Middleware solution designed and developed by 5GIC (depicted as 5GIC Exchange – 5GICE – in Figure 13) which is in charge of enabling deployment of virtual network services by users of the system, and on more than one connected testbed at a

time. In 5GIC, the virtualisation data centre has been connected to this Middleware as a Core Network testbed. 5GIC is developing solutions to achieve a fully autonomous network to derive E2E operations, integrated with artificial intelligence solutions.

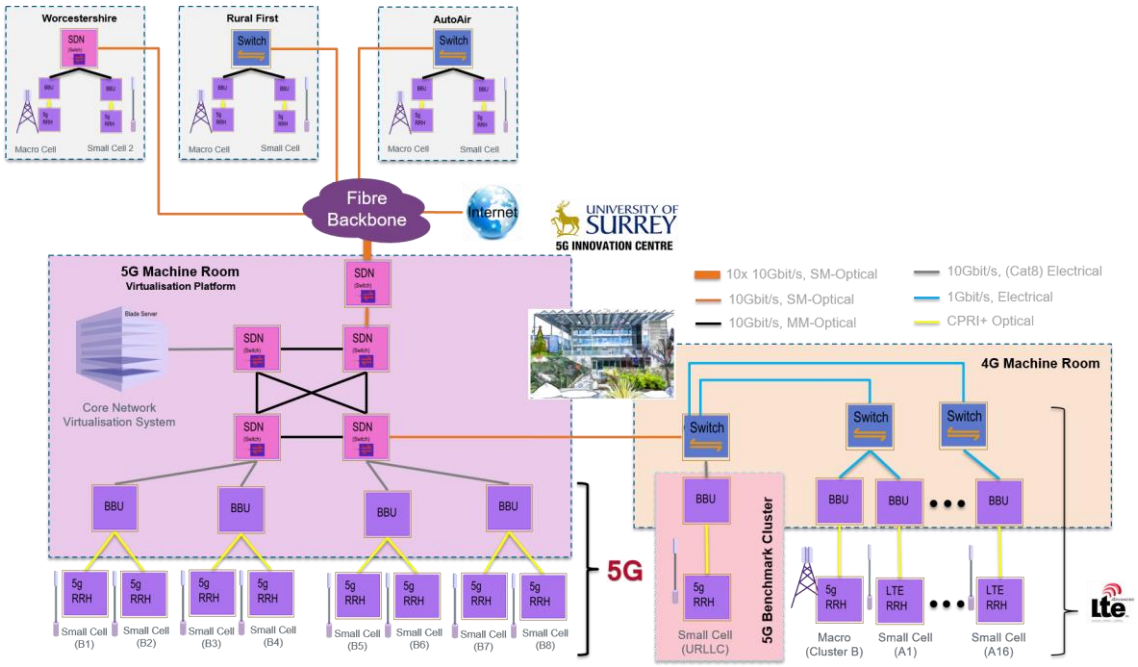

Figure 14. Logical connectivity architecture of the 5GIC testbed's integration with Worcestershire, 5G RuralFirst and Millbrook testbeds.

Network slices

Each core network instance is made available as a network slice. Control Plane Node (CPN) slices are formed as either a *common* control plane node slice consisting of the AMF, UDM and AUSF, or as a user plane control (UPc) slice that includes PCF and SMF. The User Plane Node (UPN) slices support secure MEC services via local break-out points and can also provide Internet services. All these components and their interfaces comply with the 3GPP systems architecture [9].

Connectivity backbone and the Radio access network

The 5GIC testbed has integrated SDN in its connectivity infrastructure and supports dedicated 10Gbps connections to each of the other testbeds via its fibre interconnection point on site. In total, the testbed supports up 10x 10Gbps connections, enabling further extension of the 5G eco-system, with additional testbeds.

The testbed has deployed 8x 5G NR RRHs as small cells, operating at 3.5GHz. This is in addition to the macro cell connectivity provided by 700MHz 5G NR systems deployed on University of Surrey campus, as well as the indoor and outdoor 4G RAN. The testbed is designed to support 3GPP use cases, i.e. URLLC, eMBB, and mIoT. 4G and 5G virtual core networks run in parallel, hosted in dedicated data centres, as a demonstrated deployment of orchestrated virtual network deployment. High speed fibre links connect the data centres.

4.3 Standards developing organisations, forums, industry alliances, and research projects on 5G security

Various standards developing organisations and industry alliances have been working on defining the security mechanisms and protocols for 5G networks and systems. These organisations focus on different aspects of security in mobile networks. Industry forums also have various initiatives to ensure security and user privacy.

The efforts by these bodies can be summarised as follows. Please note that this is not an all-inclusive list.

4.3.1. The Third Generation Partnership Project (3GPP)

Since 2015, 3GPP has been developing 5G standards from different perspectives, e.g. services and requirements (SA1) [43], architecture (SA2) [44], and security (SA3) [45]. The SA1 group have defined the 5G use cases as listed in Section 1, and the SA2 group have defined the systems architecture [9], which involves new radio access technologies, non-3GPP access, and the evolved LTE, besides the core network.

3GPP SA3 group have defined the security architecture for 5G networks in the specification document TS 33.501 [27]. The document also includes System Architecture Evolution (SAE) security architecture and non-3GPP security. Convergence of wireless and wireline architectures regarding security are covered in TS 33.807 [46].

The authentication framework and Network Domain Security (NDS) are covered for IPsec and DTLS in TS 33.210 [35], and TS 33.310 [29], respectively. The working group has a separate specification in the pipeline, TS 33.835 [47], which will be dedicated for authentication centre considerations for applications in 5G [47].

3GPP SA3 have also published various other specifications on Lawful Interception (LI) TS 33.842 [48], network slicing security on management TS 33.811 [49] and enhancement TS 33.813 [50], security assurance specifications in various system components (i.e. TS 33.511 for gNB [51], TS 33.512 for AMF [52], TS 33.513 for UPF [53], TS 33.514 for UDM [54], and TS 33.515 for SMF [55]), among others. The full list of specifications can be found at [56].

- 3GPP SA3 working group

This working group [57] specifies security and privacy requirements, as well as architectures and protocols for 5G security. The working group also ensures the availability of cryptographic algorithms which need to be part of the specifications. In SA3, the lawful interception (LI) working sub-group provide the requirements and specifications for lawful interception in 3GPP systems [48].

4.3.2. The European Telecommunications Standards Institute (ETSI)

ETSI has various working groups that address various aspects of security, such as information security indicators, mobile/wireless systems, IoT and M2M, network functions virtualisation, intelligent transport systems and maritime communications, broadcasting, lawful interception and retained data, digital signatures and trust service providers, smart cards and secure

elements, and security algorithms. ETSI organises annual security week events, called the ETSI Security Week, which brings security experts to study and discuss cybersecurity challenges of the digital world.

- ETSI NFV SEC

The NFV SEC sub-group [58] focuses on security considerations in NFV systems. NFV security is particularly relevant to 5G, as NFV systems and solutions are envisioned to be heavily used in 5G systems to run virtualised network services, including the mobile core and MEC services. The group is active in developing specifications for NFV security, covering hardware and software issues, identity management, authentication, authorisation, and monitoring [25]. Relevant activities of the group are on identification of security problems, threat surfaces and vulnerabilities, and requirement analysis. Of particular interest is open-source infrastructure controllers, ETSI Management and Orchestration security [59], and the like.

Besides ETSI NFV SEC, there are other subgroups, such as ETSI NFV IFA (Interfaces and Architecture), SOL (Solutions), TST (Testing, implementation, and open source), whose work on NFV is related to security in NFV systems.

- ETSI CYBER

The CYBER security working group [60] has been focusing on identifying security requirements towards standardisation. Of particular interest is privacy assurance in the context of 5G systems, covering mobile devices, mobile services, and cloud systems. This involves encryption, decryption, and key distribution. Besides the standardisation work within the group, ETSI CYBER also works on Middlebox Security Protocol, Attribute-Based Encryption, and Quantum-Safe Cryptography.

- ETSI MEC

ETSI MEC [61] is an industry specification group within ETSI that aims to make it efficient and seamless for application providers, equipment vendors, and service providers, and any third parties to integrate their solutions with the MEC systems provided by network operators. This opens up easier integration of cloud networking technologies with mobile RAN.

- ETSI LI

Lawful intercept [62] is a working group that defines standards that define legal official access procedures to private communications, against crime prevention, to be provided by service providers or network operators. This committee publishes material on Lawful Interception (LI) architectures and handover standards, with the goal of meeting international requirements and national regulations for LI in a way which is lawful, auditable, proportionate, and secure.

- ETSI Broadcast

The technical community ETSI Broadcast [63] is defining security features related with broadcast services. Some of the outcomes of the groups are the common scrambling algorithm, TV-Anytime specifications, and currently on specifications for satellite distribution systems to protect user identity and location and prevent unauthorised access.

- ETSI SES

Satellite Earth Stations and Systems (SES) [64] committee produces specifications on network security in satellite systems for broadband multimedia services. It is also concerned with the security of the satellite radio interfaces.

- ETSI SAGE

This group called the Security Algorithms Group of Experts [65] provides ETSI's cryptographic algorithms and protocols specific to fraud prevention, user data privacy assurance, and prevention of unauthorised network access.

4.3.3. The Institute of Electrical and Electronics Engineers (IEEE)

IEEE 5G Initiative, which has now been rebranded as IEEE Future Networks [66] organises 5G World Forum events to examine key critical 5G innovations across technologies, with a dedicated track on 5G security. The event attracts industry practitioners, researchers and academia, government regulators, and public sector executives.

4.3.4. Internet Engineering Task Force (IETF)

IETF [67] has focused on IoT device security with special focus groups, and has produced a use case document RFC 7744 [68], which presents a collection of representative use cases for authentication and authorization in constrained environments.

IETF Interface to Network Security Functions (I2NSF) [69] aims to define a set of software interfaces and data models to the network security functions (NSF) which may be hosted at different locations. NSFs could be services that consist of different security products from different vendors and provided by physical or virtualised infrastructure of various organisations. This diversity calls for standard interfaces to monitor, control, and consume security functions, and interact with blocks that provide security policies and rules.

4.3.5. Trusted Computing Group (TSG)

The Trusted Computing Group (TSG) [70] is a non-profit organisation that aims to enable the benefits of trust in computing devices from mobile to embedded systems, which includes networks, storage, infrastructure, and cloud security. Today, many devices, such as PCs and servers, are equipped with Trusted Platform Module (TPM). Networking devices deploy specifications on self-encryption and network security. Since May 2015, ETSI and TSG have a memorandum of understanding to establish cooperation on telecommunications standards, with the aim to work towards a secure global telecommunications infrastructure.

4.3.6. Next Generation Mobile Networks (NGMN)

NGMN [71] has been involved in definition of 5G requirements and design principles, future use cases and business models [72]. The 5G Security group has set out objectives and guides for standardisation on implementation of 5G security, with focus on architecture, IoT, platform availability, virtualisation, and privacy. The groups has published white papers on vehicle-to-infrastructure [73], 5G security for MEC [74], and network capability exposure [75].

4.3.7. GSM Alliance (GSMA)

The GSM Alliance's [76] vision for 2020 includes creation of a network for secure, smart, and seamless services. Towards this, the group published a white paper [10] on technology enablers for 5G, as part of its vision for Network 2020.

- Fraud and Security Group (FASG)

FASG [77] has been established to drive the industry's management of fraud and security matters related to GSM. It covers a wide range of topics, e.g. networks and services, protection of mobile operator technology and infrastructure as well as customer identity and privacy. This is also aimed to build trust relations, especially to improve mobile operators' reputation in the industry. The group continuously monitors security threats and analyses associated risks for network operators. It also specifies technical solutions against fraud prevention and security assurance. It also defines requirements and minimum standards for the industry to drive implementation.

4.3.8. Internet of Things Security Foundation (IoTSF)

Internet of Things Security Foundation (IoTSF) [78] is a non-profit organisation that is dedicated to security for Internet of Things (IoT). It has working groups on certification, best practices guides, compliance validation and test, vulnerability disclosure guidance, security landscape, smart buildings, and trust. Certification for IoT devices aims to have low-cost, accessible, and readily available systems of self-certification and third-party certifications.

4.3.9. Open Mobile Alliance (OMA)

Open Mobile Alliance (OMA) is an industry forum that develops open standards for the mobile phone industry. OMA SpecWorks [79] has published specifications on various topics related with security, such as application layer security common functions, authorisation framework for network APIs, identity management framework, light-weight Machine-to-Machine (LwM2M) security, mobile spam reporting, on-board key generation, secure content exchange, secure content identification mechanism, secure user plane location, secure removable media, and wireless public key infrastructure.

4.3.10. National Cyber Security Centre (NCSC)

NCSC [80] in the UK provides advice and support on how to avoid cyber-security threats. It publishes weekly reports on cyber threats, attacks, and vulnerabilities. NCSC targets at ensuring a secure and resilient national communications infrastructure.

4.3.11. International Telecommunications Union (ITU)

ITU published a paper [81] in early 2018, which outlines a set of principles on the development, establishment, and implementation of national cyber-security strategies, and is intended to be a guide to national leaders and policy-makers to develop, establish, and implement national cyber-security strategies world-wide. This involves identifying stakeholders, assessing the cyber-risk landscape. The paper outlines the processes to achieve a planned implementation of threat mitigation technologies and monitoring and evaluation of these processes. Special focus is given to critical communications infrastructure and services.

The ITU white paper titled "Setting the Scene for 5G: Opportunities & Challenges" [1] outlines 5G evolution and what it can deliver and its benefits. The paper lists the key challenges and requirements and emphasises the need for coordination of industry verticals.

4.3.12. 5G Alliance for Connected Industries and Automation (5G-ACIA)

5G-ACIA [82] is an industry forum to discuss technical, regulatory and business aspects of 5G for the industrial domain, covering industrial automation, information and communication technology, academia, and authorities. The forum published a white paper titled "5G for Connected Industries and Automation", which provides an overview of 5G's potential for the automation industry, and the use cases and requirements. The document highlights the need for security mechanisms for Industry 4.0 communication systems as they are connected to 5G mobile networks and systems. Logical attacks are mentioned to be in the form of side-channel analysis of interfaces and exploitation implementation weaknesses. Physical attacks are in the form of tampering/hacking Industry 4.0 devices, ultimately exploiting device identity and keys. It is noted that both logical and physical attacks could be performed in an automated way, which requires local and remote management of devices and security mechanisms. Finally, it is noted that device authenticity now means company identity, which is important to protect to avoid industry espionage scenarios.

4.3.13. 5G Automotive Association (5GAA)

5GAA [83] is a global organisation of companies from various industry sectors related with automotive technology and communications, with the goal to develop end-to-end solutions. It has the goal to achieve cooperative intelligent transport systems (C-ITS) which is for vehicles to share information for safer, greener, more enjoyable transport. 5GAA considers 5G mobile networks to be the key player to realise C-ITS, especially for mission-critical communications, and connected mobility scenarios.

4.3.14. British Security Industry Association (BSIA)

BSIA [85] is the trade association for professional security industry in the UK. Members of this organisation provide UK security services and products, which includes distribution and installation of physical security equipment.

4.3.15. Small Cell Forum

Small Cell Forum (SCF) [86] is an industry forum targeting at accelerating small cell deployments. To achieve this, SCF works with regulators and municipalities towards removing commercial and technical barriers, and partners with enterprises to forge new business cases. It has partnerships with ETSI, 3GPP, NGMN, GSMA, and Wireless Broadband Alliance.

4.3.16. Wireless Broadband Alliance

Wireless Broadband Alliance (WBA) [87] aims to resolve business issues to enable collaborative opportunities for service providers, enterprises and cities, enabling them to enhance the customer experience on Wi-Fi and significant adjacent technologies. WBA focused on how Wi-Fi and other unlicensed technologies can play a key role in enabling those under 5G framework, include assessing the approaches of how to integrate Wi-Fi and 5G.

4.3.17. Communications Security, Reliability, and Interoperability Council (CSRIC)

CSRIC is a council under the US Federal Communications Communication (FCC), provides FCC with recommendations on optimal security and reliability of communications systems, including telecommunications, media, and public safety. It has recently published a technical report [88] on guidelines for mitigating security risks of emerging 5G networks.

4.3.18. 5G Americas

5G Americas is an industry trade organisation of service providers and manufacturers and is aimed at developing 5G for the Americas. The organisation published a white paper [89] titled "The Evolution of Security in 5G", which covers information on 3GPP 5G security standards, 5G threat surface, and DDoS attack mitigation. The threat surfaces mentioned in the paper are IoT and massive IoT, UE, RAN, core, network slicing, SDN and NFV, subscriber privacy, and interworking and roaming threats.

Besides the ones presented above, there are many other organisations whose work is related with 5G networks, 5G security, or the security of systems anticipated to interconnect or internetwork with 5G networks. Some of these organisations are National Institute of Standards and Technology (NIST) [90], Telecommunications Infrastructure Project (TIP) [91], Global Certification Forum [92] and Telecommunications Technology Association [93].

4.3.19. EU 5G PPP Research Projects

5G PPP, the 5G Public Private Partnership research initiative by the European Commission and Europe ICT industry, has been running three phases of research projects, some of which had a security focus for the next generation communication networks and services. It has a vision for secure, reliable, and dependable network that enables advanced user-controlled privacy. 5G-PPP published a white paper on 5G security landscape in July 2017 [20], which outlines 5G security from various perspectives, i.e. risks, requirements, architecture, monitoring and management, access control, privacy and trust, and standardisation.

The following is a selected set of research projects that have focused on 5G security aspects during the three phases of the 5G PPP programme so far.

- 5G-ENSURE

This project [95], called 5G Enables for Network and System Security and Resilience, analysed potential security threats and requirements in 5G systems, and significantly contributed to the 5G PPP Security white paper [20]. This involves services, security architecture, as well as access networks, authentication, privacy, and network slicing. The project provided input to 3GPP SA3, and also covers user privacy and identity protection mechanisms defined by ETSI CYBER.

- CHARISMA

The Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access (CHARISMA) [96] project emphasizes that 5G will bring new business, trust, and service delivery models, with increased privacy concerns with an evolved threat landscape. These are attributed to convergence of big data with 5G, making 5G networks a critical infrastructure itself. The project also notes [97] that the variety of communication technologies deployed on UEs, increased levels of data transmission, and existence of mobile malware and botnets will make UEs more open to attack.

- 5G-MoNArch

The 5G-MoNArch project (5G Mobile Network Architecture for diverse services, use cases, and applications in 5G and beyond) [98] has a work item on resilience and security, which focuses on key functional innovations required for different use cases from a security perspective.

- Internet of Radio Light (IoRL)

This project [99] aims to develop safer, more secure, customisable and intelligent network for indoor communications.

- NRG-5

This project [100] is focused on theme of enabling smart energy as a service via 5G mobile network advances. The project has a goal to deliver a decentralised, secure, and resilient

framework, focusing on high availability of services for hardware constrained devices, edge computing scenarios and virtualisation of services for energy utility infrastructures.

- SLICENET

SLICENET [101] is a project on end-to-end cognitive network slicing and slice management framework in virtualised multi-domain, multi-tenant 5G networks. The project focused on E2E slicing through mechanisms such as slice-provisioning, control, management, and orchestration. Cognitive network management and orchestration engines are to take into account security as well as performance.

- 5G-DRIVE

5G-DRIVE [102] is an EU-China collaboration project targeted at eMBB and Internet of Vehicles (IoV) trials, including V2X and MEC use cases. The project has work items on network and terminal security.

Bibliography

[1] DCMS 5G Testbeds and Trials Programme (5G T&T), https://www.gov.uk/government/collections/5g-testbeds-and-trials-programme

[2] "Setting the scene for 5G: Opportunities & Challenges", ITU report, 2018, available at https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf

[3] Feasibility study on new services and markets technology enablers for enhanced mobile broadband; Stage 1, 3GPP technical specification TS 22.863, http://www.3gpp.org/ftp//Specs/archive/22_series/22.863/

[4] Feasibility study on new services and markets technology enablers for critical communications; Stage 1, 3GPP technical specification TS 22.862, http://www.3gpp.org/ftp//Specs/archive/22_series/22.862/

[5] FS_SMARTER - massive Internet of Things, 3GPP technical specification TS 22.861, http://www.3gpp.org/ftp//Specs/archive/22_series/22.861/

[6] "Software-Defined Networking: A Comprehensive Survey", Diego Kreutz, Fernando M. V. Ramos, Paulo Esteves Veríssimo, Christian Esteve Rothenberg, Siamak Azodolmolky, Steve Uhlig, *Proceedings of the IEEE*, vol 103, no 1, pp 14-76, January 2015,

[7] "Network Function Virtualisation: State-of-the-Art and Research Challenges", Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck, Raouf Boutaba, *IEEE Communications Surveys & Tutorials*, vol 18, no 1, 236-262, September 2015,

[8] "Network Functions Virtualisation— Introductory White Paper", ETSI, 22 October 2012, retrieved 20 June 2013.

[9] TS 23.501, System Architecture for the 5G System, 3GPP, http://www.3gpp.org/ftp//Specs/archive/23_series/23.501/

[10] "Unlocking commercial opportunities – from 4G evolution to 5G", GSMA, March 2017, https://www.gsma.com/futurenetworks/wp-content/uploads/2017/03/704_GSMA_unlocking_comm_opp_report_v5.pdf

[11] Multi-access edge computing, https://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing, accessed 13 November 2018.

[12] "Flat Distributed Cloud (FDC) architecture", 5G Innovation Centre, https://www.surrey.ac.uk/sites/default/files/5G-Network-Architecture-Whitepaper-(Jan-2016).pdf

[13] TR 28.801, "Study on management and orchestration of network slicing for next generation network", 3GPP, http://www.3gpp.org/ftp//Specs/archive/28_series/28.801/

[14] 5G Innovation Centre, University of Surrey, http://www.surrey.ac.uk/5gic

[15] TS 23.502, Procedures for the 5G System, 3GPP, http://www.3gpp.org/ftp//Specs/archive/23_series/23.502/

[16] REST, REpresentational State Transfer, https://restfulapi.net/

[17] GS-NFV-SEC-011, "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture", v1.1.1, ETSI NFV-SEC, April 2018, accessed 4 November 2018.

[18] GS NFV-SEC-009, “Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration”, ETSI NFV SEC, December 2015, accessed 4 November 2018.
[19] GS-NFV-SEC-010, “Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements”, v1.1.1, ETSI NFV-SEC, April 2016, accessed 4 November 2018.
[20] “5G PPP Phase 1 Security Landscape”, 5G PPP Security WG, June 2017, available at https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf, accessed on 5 November 2018.
[21] GS NFV-SEC-019, “Network Functions Virtualisation (NFV) Release 3; Security; System Architecture Specification for NFV Security Enhancements - Architecture for Sec enhancement Spec ”, ETSI NFV SEC, Early Draft, 20 September 2018, accessed 4 November 2018.
[22] GS NFV-SEC-012, “Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components”, v3.1.1, ETSI NFV SEC, January 2017, accessed 4 November 2018.
[23] GS NFV-IFA-026, “Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Architecture enhancement for Security Management Specification - Architecture enhancement for Sec Mgmt Spec”, ETSI NFV IFA, Early Draft, 19 September 2018, accessed 4 November 2018.
[24] GS NFV-IFA-033, “Network Functions Virtualization (NFV) Release 3; Management and Orchestration; Sc-Or, Sc-Vnfm, Sc-Vi reference points - Interface and Information Model Specification SEC-MANO ref points - Intface Spec”, ETSI NFV IFA, Early Draft, 25 October 2018, accessed 4 November 2018.
[25] GS NFV-SEC-013, “Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification”, v3.1.1, ETSI NFV SEC, February 2017, available at https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/013/03.01.01_60/gs_NFV-SEC013v030101p.pdf, accessed 4 November 2018.
[26] GSTR-TN5G, “Transport Network Support of IMT-2020/5G”, ITU-T Technical Report, February 2018, https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-HOME-2018-PDF-E.pdf
[27] TS 33.501, Security architecture and procedures for 5G System, 3GPP, http://www.3gpp.org/ftp//Specs/archive/33_series/33.501/
[28] 3GPP TS 33.210, “Network Domain Security (NDS), IP network layer security”.
[29] TS 33.310, Network Domain Security (NDS), Authentication framework, 3GPP, http://www.3gpp.org/ftp//Specs/archive/33_series/33.310/
[30] 3GPP TS 33.310, "Network Domain Security (NDS); Authentication Framework (AF)".
[31] IETF RFC 5448, " Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".
[32] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".
[33] “Overview of 5G Security”, X. Zhang, A. Kunz, and S. Schröder, IEEE Conference on Standards for Communications and Networking (CSCN), 2017.

[34] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".
[35] TS 33.210, IP network layer security, 3GPP, http://www.3gpp.org/ftp//Specs/archive/33_series/33.210/
[36] 5GIC member network, https://www.surrey.ac.uk/5gic/members/network
[37] IETF RFC 6749: "OAuth2.0 Authorization Framework".
[38] OpenStack open source cloud computing software, https://www.openstack.org/
[39] ETSI OSM, an Open Source NFV Management and Orchestration (MANO) software stack aligned with ETSI NFV, https://osm.etsi.org/
[40] ETSI MANO specification, http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf
[41] OpenDaylight, https://www.opendaylight.org/
[42] Ryu, a component-based software defined networking framework, https://osrg.github.io/ryu/
[43] 3GPP Study Area 1 (SA1) - Services, http://www.3gpp.org/specifications-groups/sa-plenary/sa1-services
[44] 3GPP Study Area 2 (SA2) - Architecture, http://www.3gpp.org/specifications-groups/sa-plenary/sa2-architecture
[45] 3GPP Study Area 3 (SA3) - Security, http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security
[46] TS 33.807, “Study on the security of the wireless and wireline convergence for the 5G system architecture”, 3GPP, Release 16, http://www.3gpp.org/ftp//Specs/archive/33_series/33.807/
[47] TS 33.835, “Study on authentication and key management for applications based on 3GPP credential in 5G”, 3GPP, Release 16.
[48] TS 33.842, “Study on Lawful Interception (LI) service in 5G”, 3GPP, Release 15, http://www.3gpp.org/ftp//Specs/archive/33_series/33.842/
[49] TS 33.811, “Study on security aspects of 5G network slicing management”, 3GPP, Release 15, http://www.3gpp.org/ftp//Specs/archive/33_series/33.811/
[50] TS 33.813, “Study on security aspects of network slicing enhancement”, 3GPP, Release 16.
[51] TS 33.511, “5G Security Assurance Specification (SCAS); NR Node B (gNB)”, 3GPP, Release 16, http://www.3gpp.org/ftp//Specs/archive/33_series/33.511/
[52] TS 33.512, “5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)”, 3GPP, Release 16, http://www.3gpp.org/ftp//Specs/archive/33_series/33.512/
[53] TS 33.513, “5G Security Assurance Specification (SCAS); User Plane Function (UPF)”, 3GPP, Release 16, http://www.3gpp.org/ftp//Specs/archive/33_series/33.513/
[54] TS 33.514, “5G Security Assurance Specification (SCAS); Unified Data Management (UDM)”, 3GPP, Release 16, http://www.3gpp.org/ftp//Specs/archive/33_series/33.514/
[55] TS 33.515, “5G Security Assurance Specification (SCAS); Session Management Function (SMF)”, 3GPP, Release 16, http://www.3gpp.org/ftp//Specs/archive/33_series/33.515/
[56] 3GPP specification series on security, http://www.3gpp.org/DynaReport/33-series.htm

[57] 3GPP SA3, working group on security and privacy in 3GPP systems, http://www.3gpp.org/Specifications-groups/sa-plenary/54-sa3-security
[58] ETSI standards working group on NFV, https://www.etsi.org/technologies-clusters/technologies/nfv
[59] GS NFV-SEC-014, "Security specification for MANO components and reference points", v3.1.1, April 2018, available at https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/014/03.01.01_60/gs_NFV-SEC014v030101p.pdf, accessed 8 November 2018.
[60] ETSI standards working group on cyber security, https://www.etsi.org/technologies-clusters/technologies/cyber-security
[61] ETSI MEC industry specification group, https://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing, accessed 4 November 2018.
[62] Lawful Intercept, https://www.etsi.org/technologies-clusters/technologies/lawful-interception
[63] ETSI Broadcast industry specification group, https://www.etsi.org/technologies-clusters/technologies/broadcast
[64] ETSI Satellite Earth Stations and Systems (SES), https://www.etsi.org/technologies-clusters/technologies/satellite
[65] ETSI Security Algorithms, https://www.etsi.org/technologies-clusters/technologies/security-algorithms
[66] IEEE Future Networks – enabling 5G and beyond, https://futurenetworks.ieee.org/about, accessed on 6 November 2018.
[67] IETF, Internet Engineering Task Force, https://www.ietf.org/
[68] RFC 7744, "Use Cases for Authentication and Authorization in Constrained Environments", IETF, https://tools.ietf.org/pdf/rfc7744.pdf
[69] RFC 8192, "Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases" IETF, https://tools.ietf.org/pdf/rfc8192.pdf
[70] Trusted Computing Group, https://trustedcomputinggroup.org/, accessed 6 Nov. 2018.
[71] NGMN – Next Generation Mobile Networks, https://ngmn.org/home.html
[72] NGMN 5G White Paper, https://www.ngmn.org/5g-white-paper/5g-white-paper.html
[73] "V2X White Paper", NGMN Alliance, 17 June 2018, https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/V2X_white_paper_v1_0.pdf, accessed 7 November 2018.
[74] "Mobile Edge Computing / Low Latency / Consistent User Experience", v2.0, 20 Feb. 2018, https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/180220_NGMN-5G_Security_MEC_ConsistentUExp_v2.0.pdf
[75] "Security aspects of network capabilities exposure in 5G", NGMN Alliance, 21 Sep. 2018, https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2018/180921_NGMN-NCEsec_white_paper_v1.0.pdf
[76] GSMA - Global System for Mobile communications Association, https://www.gsma.com/
[77] GSMA Fraud and Security Group, https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group, accessed on 6 November 2018.

[78] IoT Security Foundation (IoTSF), https://www.iotsecurityfoundation.org/working-groups/, accessed on 6 November 2018.
[79] OMA SpecWorks, https://www.omaspecworks.org/, accessed on 6 November 2018.
[80] National Cyber Security Centre, https://www.ncsc.gov.uk/
[81] "Guide to developing a national cybersecurity strategy", International Telecommunication Union, 2018, available at http://www.itu.int/pub/D-STR-CYB_GUIDE.01-2018, accessed on 8 November 2018.
[82] 5G Alliance for Connected Industries and Automation (5G-ACIA), https://www.5g-acia.org/, accessed on 8 November 2018.
[83] 5G Automotive Association (5GAA), http://5gaa.org/, accessed on 8 November 2018.
[84] "5G for connected industries and automation", 5G-ACIA, April 2018, available at https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/Whitepaper_5G_for_Connected_Industries_and_Automation/5G-for-Connected-Industries-and-Automation-White-Paper.pdf, accessed on 8 November 2018.
[85] British Security Industry Association (BSIA), https://www.bsia.co.uk/
[86] Small Cell Forum, https://www.smallcellforum.org/
[87] Wireless Broadband Alliance, https://www.wballiance.com/
[88] "Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks", v14.0, US Federal Communications Commission, September 2018, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council, accessed 6 November 2018.
[89] "The evolution of security in 5G", 5G Americas, October 2018, available at http://www.5gamericas.org/files/8815/4092/3086/5G_Americas_5G_Security_White_Paper_Final.pdf, published on 8 November 2018.
[90] National Institute of Standards and Technology (NIST), https://www.nist.gov/
[91] Telecommunications Infrastructure Project (TIP), https://telecominfraproject.com/
[92] Global Certification Forum, https://www.globalcertificationforum.org/
[93] Telecommunications Technology Association, https://www.tta.or.kr/English/
[94] 5G PPP, https://5g-ppp.eu/
[95] 5G PPP Ensure project, https://5g-ppp.eu/5g-ensure/
[96] 5G PPP Charisma project, https://5g-ppp.eu/charisma/
[97] "Security and privacy challenges in 5G networks", available at http://www.charisma5g.eu/wp-content/uploads/2016/07/Security-and-privacy-challenges-in-5G-networks.pdf, accessed 10 November 2018.
[98] 5G PPP Monarch project, https://5g-monarch.eu/
[99] 5G PPP Internet of Radio-Light in Buildings project, https://5g-ppp.eu/wp-content/uploads/2017/06/IoRL-5GPPP-v01-4.pdf
[100] 5G PPP NRG-5 project, http://www.nrg5.eu/
[101] 5G PPP SLICENET project, https://slicenet.eu/
[102] EU 5G-DRIVE project, https://5g-drive.eu/

List of Acronyms and Abbreviations

Acronym	Meaning
3GPP	Third Generation Partnership Project
4G	Fourth Generation Mobile Network
5G	Fifth Generation Mobile Network
5GIC	5G Innovation Centre
5GICE	5GIC Exchange
5G NR	5G New Radio
5GPPP	5G infrastructure Public Partnership Project
5GRF	5G RuralFirst
5G UE	5G User Equipment
AAA	Authentication, Authorisation, Accounting
AF	Application Function
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
AMF	Access and Mobility Function
AN	Access Network
API	Application Programming Interface
AR	Augmented Reality
ARPF	Authentication credential Repository and Processing Function
AUSF	Authentication Server Function
BBU	Base Band Unit
CAPIF	Common API Framework
CAV	Connected Autonomous Vehicles
CP	Control Plane
CPN	Control Plane Node
CPU	Central Processing Unit
C-RAN	Cloud Radio Access Network
CU	Central Unit
CUPS	Control and User Plane Separation
DCMS	Department for Digital, Culture, Media & Sport
DDoS	Distributed Denial of Service
D-RAN	Distributed RAN
DTLS	Datagram Transport Layer Security
DU	Distributed Unit
E2E	End-to-End
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data rates for GSM Evolution
eMBB	enhanced Mobile Broadband
eNodeB	evolved NodeB
EPC	Evolved Packet Core

ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FDC	Flat Distributed Cloud
gNB	Next Generation NodeB
GSM	Global System for Mobile communications
GUTI	Globally Unique Temporary Identifier
HE	Home Environment
HSS	Home Subscriber Server
HW	HardWare
I2NSF	Interface to Network Security Functions
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IMT	International Mobile Telecommunications
IoT	Internet of Things
IoTSF	Internet of Things Security Foundation
IP	Internet Protocol
IPX	Internetwork Packet eXchange
IT	Information Technology
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LAN	Local Area Network
LI	Lawful Intercept
LiFi	Light Fidelity
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
M2M	Machine-to-Machine
MANO	Management and Orchestration
ME	Mobile Equipment
MEC	Multi-access Edge Computing
MHSP	Malvern Hills Science Park
MitM	Man-in-the-Middle
mIoT	Massive Internet of Things
mmWave	millimeter Wave
MME	Mobility Management Entity
MNO	Mobile Network Operator
MR	Mixed Reality
MTC	Machine Type Communications
mMTC	massive Machine Type Communications
NAS	Non-Access Stratum
NaaS	Network as a Service

NB-IoT	Narrow-Band Internet of Things
NDS	Network Domain Security
NEF	Network Exposure Function
NFV	Network Functions Virtualisation
NGMN	Next Generation Mobile NetworksI2
NRF	Network Repository Function
NS	Network Service
NSA	Non-Stand-Alone
NSSF	Network Slice Selection Function
OAM	Operations And Maintenance
OMA	Open Mobile Alliance
OSI	Open Systems Interconnection
OSM	Open Source Mano
OTA	Over-The-Air
PCF	Policy Control Function
PDA	Personal Digital Assistant
PDN	Packet Data Network
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PGW	PDN Gateway
PGWc	PGW control
PGWu	PGW user plane
QoS	Quality of Service
RAN	Radio Access Network
RAT	Random Access Technology
REST	REpresentation State Transfer
RF	Radio Frequency
RRC	Radio Resource Control
RRH	Remote Radio Head
RTT	Round Trip Time
RU	Radio Unit
SA	Stand Alone
SAE	System Architecture Evolution
SBA	Service Based Architecture
SDN	Software Defined Network
SDO	Standards Developing Organisations
SEAF	SEcurity Anchor Function
SEG	SEcurity Gateway
SEPP	Security Edge Protection Proxy
SGW	Serving Gateway
SGWc	SGW control
SGWu	SGW user plane

SIDF	Subscription Identifier De-concealment Function
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SME	Small and Medium-sized Enterprises
SMF	Service Management Function
SN	Secondary Network
SNMP	Simple Network Management Protocol
SUCI	SUbscription Concealed Identifier
SUPI	SUbscription Permanent Identifier
SYS	SYStem
SW	SoftWare
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDM	User Data Management
UE	User Equipment
UK	United Kingdom
UP	User Plane
UPc	User Plane control
UPF	User Plane Function
UPN	User Plane Node
URLLC	Ultra-Reliable and Low Latency Communications
USIM	Universal Subscriber Identity Module
V2I	Vehicle to Infrastructure
V2V	Vehicle to vehicle
V-RAN	Virtual Radio Access Network
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtual Network Function
VR	Virtual Reality
WiFi	Wireless Fidelity

Contributors:

Contributor	Partner	Testbed	Role
Serdar Vural	5GIC, University of Surrey	5GIC	Lead Author and Editor
Stuart Revell	5GIC, University of Surrey	5GIC	Content contributor, Reviewer
Mark Shepherd	5GIC, University of Surrey (TenCastle)	5GIC	Content contributor
Gerry Foster	5GIC, University of Surrey	5GIC	Content contributor, Reviewer
Mark Hawkins	QinetiQ	Worcestershire	Content contributor
Gregory Lupton	QinetiQ	Worcestershire	Content contributor, Reviewer
Muquid Ali	AWTG	Worcestershire	Reviewer
Xhafer Krasniqi	Quortus	AutoAir	Content contributor, Reviewer
Peter Claydon	AirSpan	AutoAir	Content contributor, Reviewer
Steve Methley	DCMS	ALL	Observer, Reviewer
Malcolm Brew	Strathclyde	5GRF	Content contributor
Dez O'Connor	Cisco	5GRF	Content contributor, Reviewer

Disclaimer

Department for Digital, Culture Media & Sport

This project has received funding from UK Government Department for Digital, Culture, Media & Sport (DCMS).