RESERVE

D3.7 v1.0

Report on Requirements on scalable ICT to implement Voltage Control Concepts, V2

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 727481.

Project Name	RESERVE
Contractual Delivery Date:	30.09.2019
Actual Delivery Date:	30.09.2019
Contributors:	Robert Farac (EDD), Zain Mehdi (EDD), Fiona Williams (EDD), Miguel Ponce de Leon (WIT), David Ryan (WIT), Niall Grant (WIT), Darren Leniston (WIT), Sriram Gurumurthy (RWTH)
Workpackage:	WP3
Security:	PU
Nature:	R
Version:	1.0
Total number of pages:	49

Abstract:

This document is a report on the Information and Communications Technology Requirements for RESERVE and it focuses on the 5G aspects of the requirements and the potential solutions which 5G offers for these requirements.

The requirements are based on the latest RESERVE voltage control scenarios identified in D3.2 for future 100% RES penetration. It builds on the results of D3.6 and the lab tests on the 5G networks. It provides a detailed analysis of the solutions which 5G can provide in relation to the requirements.

Keyword list:

Information and Communications Technology Requirements, 100% RES Energy Networks, Voltage Control Concepts

Executive Summary

This Deliverable D3.7 presents the work of Task T3.6, “Requirement on scalable ICT to implement voltage control concepts” within the wider context of Work Package WP3 and RESERVE. WP3 focuses on the detailed analysis of the challenges and solutions for voltage control. These topics are highly relevant in future energy networks with up to 100% Renewable Energy Sources (RES).

This Deliverable D3.7 replaces and extends Deliverable D3.6 with the same aim to define the Information and Communication Technology (ICT) requirements for the voltage control scenarios. In addition, it takes into consideration the communication protocols performance tests conducted on the 5G networks in the lab. Timescales and preconditions relevant to the commercial scale use of the voltage control scenarios are described. For each of the voltage control scenarios, ICT communication solutions are provided. At the end of this deliverable, a summary of the ICT requirements is presented.

In this deliverable, ICT communications aspects of the voltage control techniques are considered with the focus on the novel fifth generation cellular network technology (5G). At the beginning of this deliverable, 5G concepts and features relevant for the voltage control are described. Afterwards, these 5G features are related to the voltage control scenarios.

Authors

Partner	Name	Phone/E-mail	
EDD			
	Robert Farac	e-mail:	robert.farac@ericsson.com
	Zain Mehdi	e-mail:	zain.mehdi@ericsson.com
	Fiona Williams	e-mail:	fiona.williams@ericsson.com
RWTH			
	Sriram Gurumurthy	e-mail:	sgurumurthy@eonerc.rwth-aachen.de
WIT			
	David Ryan	e-mail:	dryan@tssg.org
	Miguel Ponce de Leon	e-mail:	miguelpdl@tssg.org
	Niall Grant	e-mail:	ngrant@tssg.org
	Darren Leniston	e-mail:	dleniston@tssg.org

Table of Contents

1. Introduction

This Deliverable (D) 3.7 presents the final output of Task (T) 3.6, “Requirement on scalable ICT to implement voltage control concepts” replacing and expanding the requirements analysis presented previously in D3.6.

As RESERVE has a strong focus on 5G systems and their potential to support new management techniques in the power sector, the focus of the investigations of potential solutions to the requirements is on 5G cellular wireless systems. In this deliverable, we elaborate additionally on the steps that need to be taken to commercially introduce each of the new techniques as part of the general work of RESERVE on developing the exploitation of project results and also to provide a time and regulatory perspective for the solutions we propose.

1.1 Task 3.6

This deliverable is the most relevant output of Task 3.6 in WP3. This task collects and analyses the high-level capabilities of 5G-based ICT systems for voltage control. This analysis will lead to secure, resilient and scalable mechanisms for voltage control solutions for low and medium voltage distribution systems. The focus is on transmitting wide-area field measurements and control commands for these mechanisms. This report will also provide an overview of communications and energy architectures that are relevant to the lab and field trials to be executed in test beds of WP5.

1.2 Objectives of the Work Report in this Deliverable

- To provide the basis for investigating the potential role of new 5G-based ICT systems in supporting new management techniques in the power infrastructure;
- To establish a basis for providing input to 5G standardisation processes in relation to the requirements of the stakeholders as we move towards 100% RES;
- To provide the basis for investigating solutions necessary to the ICT requirements of the power sector in the 100% RES context;

1.3 Outline of the Deliverable

The document starts with an introduction to cellular wireless generations and to 5G features, in particular in Chapter 2. The definition of the ICT and 5G solutions of the energy scenarios currently in use in RESERVE for voltage control is described in Chapter 3. Chapter 4 discusses relevant general issues and conclusions of this work.

1.4 How to Read this Document

This document can be read independently, but to learn about the details of the scenarios from the electrical point of view, the authors suggest reading deliverables D3.2, D3.3, and D3.5 in parallel. Note that D3.6 defines ICT requirements that are replaced and extended in this deliverable. These documents cover both approaches for voltage control where indicated:

a) Dynamic Voltage Stability Monitoring (Sv_A; A)
b) Active Voltage Management (Sv_B; B)

Overall, this deliverable (D3.7) is related to the following documents from the RESERVE project:

- D1.3 ICT Requirements
- D3.1 Power Electronics Stability Criteria for AC Three Phase Systems (A, B)
- D3.2 Demand Response and DG control considering Voltage Control and Stability
- D3.3 Power Electronics System-level stability criteria
- D3.4 Network Impedance Characterisation for Active distribution Networks
- D3.5 Specification for an on-line system level monitoring system

The following Figure 1-1 summarises the workflow in Work Package 3, and the related input and output between related tasks and deliverables.

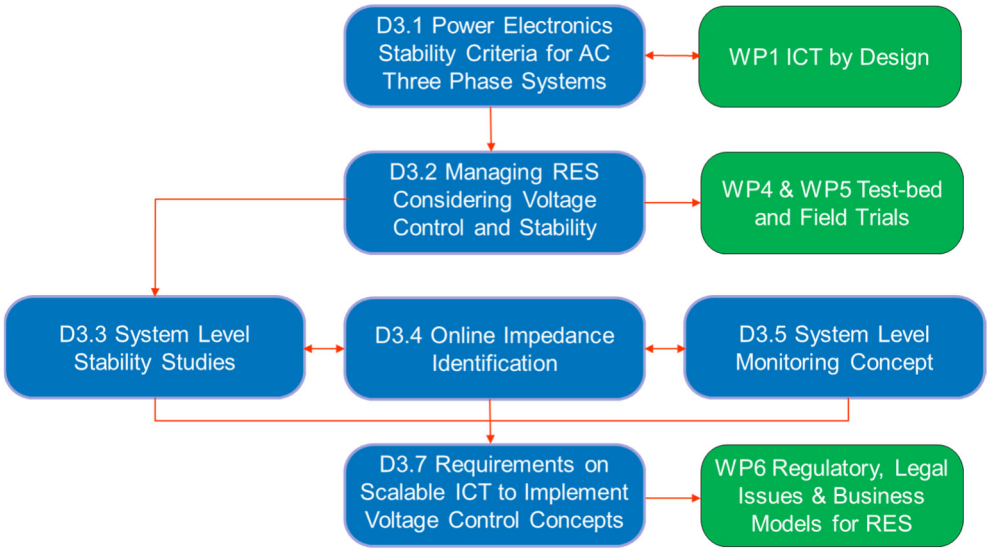

Figure 1-1 Relations between Deliverables in WP3 and other Work Packages

1.5 Approach Used to Undertake the Work

The following steps were iteratively applied to develop the results reported in this deliverable:

- A detailed investigation of the key scenarios selected in WP1 was performed with the partners active in WP3 in the project.
- A categorisation of the options for the architecture of the scenarios was developed and used later as a basis for the ICT requirements definition.
- A categorisation of the ICT potential requirements was developed as the basis for the systematic analysis of the detailed energy scenarios.
- Conclusions regarding the key ICT requirements were developed. These requirements relate to the domains of voltage and frequency control respectively.
- In addition to requirements, this document will also show some relevant ICT solutions for the requirements described.

2. 5G Cellular Wireless Systems

5G systems are the focus of RESERVE project investigations as they offer the potential to flexibly and cost-effectively support the commercial deployment of new techniques for voltage management in power networks, which will be needed to support power networks with up to 100% RES generation sources. Such new techniques were developed and elaborated in WP3 and validated through simulations in WP5 of the RESERVE project and the scenarios described in D3.6 for their use form the basis for our definition of their ICT requirements and the solutions which 5G could provide.

1.6 Evolution of mobile networks and introduction to 5G

Compared with previous generations of wireless communications technology (Figure 2-1), including 4G, the rationale for 5G development is to expand the broadband capability of mobile networks, and to provide specific capabilities not only for consumers but also for various industries and society at large, hence unleashing the potential of the Internet of Things (IoT). The overall aim of 5G is to provide ubiquitous connectivity for any kind of device and any kind of application that may benefit from being connected.

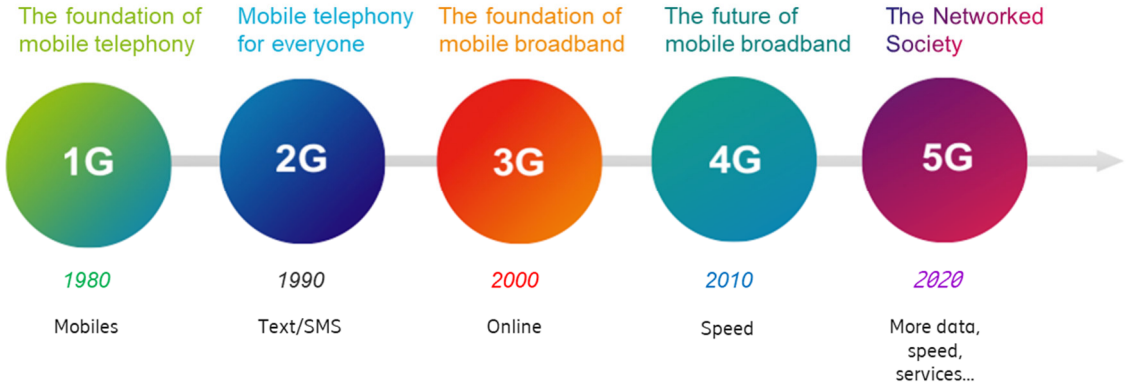

Figure 2-1 Wireless access generations

1.7 Basic 5G functionality

In order to enable connectivity for a very wide range of applications with new characteristics and requirements, the capabilities of 5G wireless access must extend far beyond those of previous generations of mobile communication. These capabilities will include massive system capacity, very high data rates everywhere, very low latency, ultra-high reliability and availability, very low device cost and energy consumption, and energy-efficient networks. Performance requirements of 5G are depicted in Figure 2-2 [7].

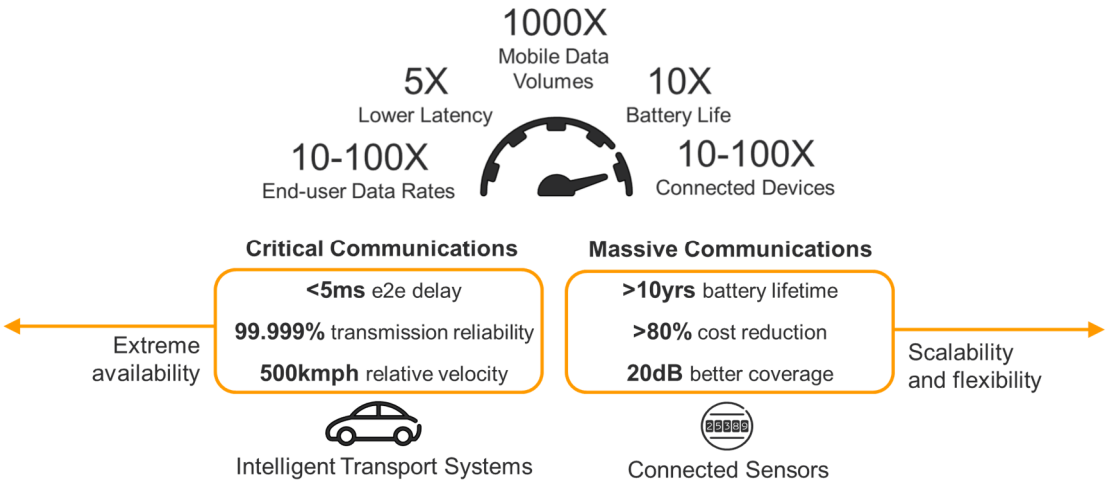

Figure 2-2 Overview of performance requirements for 5G

5G should support **data rates** exceeding 10Gbps in specific scenarios such as indoor and dense outdoor environments. **Very low latency** will be driven by the need to support new applications. Some envisioned 5G use cases, such as traffic safety and control of critical infrastructures and industry processes, require much lower latency compared with what is possible with the mobile-communication systems of today. To support such latency-critical applications, 5G should allow for an application end-to-end latency of 1ms or less. In addition to very low latency, 5G should also enable connectivity with **ultra-high reliability** and ultra-high availability. For example, some industrial applications might need to guarantee successful packet delivery within 1ms with a probability as high as 99.9999 percent. To enable the vision of billions of wirelessly connected sensors, actuators and similar devices, a further step has to be taken in terms of **device cost and energy consumption**. It should be possible for 5G devices to be available at very low cost and with a battery life of several years without recharging. **Energy efficiency on the network side** has recently emerged as an additional Key Performance Indicator (KPI).

In order to support increased traffic capacity and to enable the transmission bandwidths needed to support very high data rates. 5G will extend the range of frequencies used for mobile communication (Figure 2-3). This includes **new spectrum** below 6GHz, as well as spectrum in higher frequency bands. Frequency spectrum relevant for 5G wireless access therefore ranges from below 1GHz up to 100GHz. The specification of 5G will include the development of a new flexible air interface, New Radio (NR), which will be directed to extreme mobile broadband deployments.

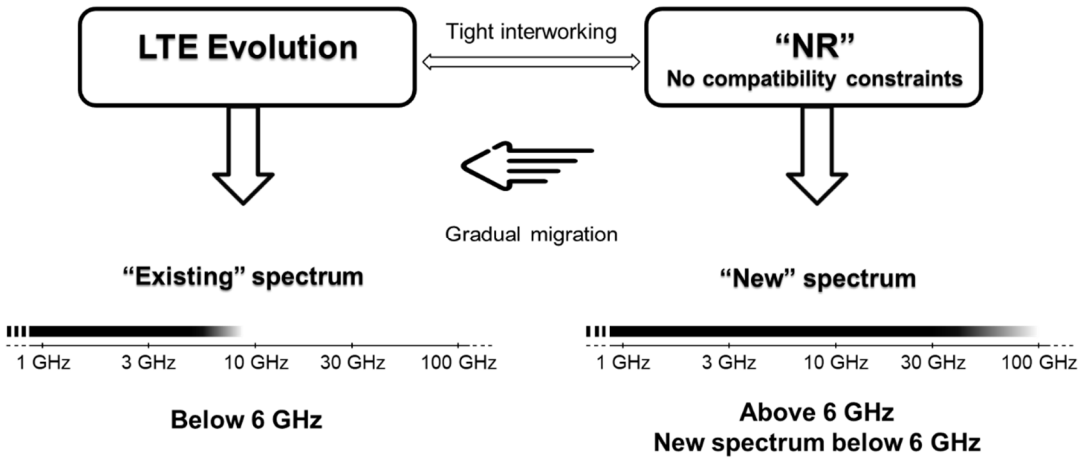

Figure 2-3 5G Frequency Spectrum for LTE Evolution and New Radio

It is important to understand that high frequencies, especially those above 10GHz, can only serve as a complement to lower frequency bands, and will mainly provide additional system capacity and very wide transmission bandwidths for extreme data rates in dense deployments. Spectrum allocations at lower bands will remain the backbone for mobile-communication networks in the 5G era, providing ubiquitous wide-area connectivity.

1.8 Cellular IoT use cases

Cellular Internet of Things (IoT) has the capability to address both the relatively simpler requirements of the Massive IoT market as well as the highly specific, sensitive demands of complex environments and applications [1]. The number of Cellular IoT connections enabled by Narrowband IoT (NB-IoT) and Long Term Evolution for Machines (LTE-M) continues to grow. The number of devices connected by Massive IoT and other emerging cellular technologies is forecast to reach 4.1 billion by 2024.

Cellular IoT itself is a rapidly growing ecosystem based on 3GPP global standards, supported by an increasing number of mobile network providers as well as device, chipset, module and network infrastructure vendors. It offers better performance than other Low Power Wide Area (LPWA) network technologies in terms of unmatched global coverage, Quality of Service, scalability, security and the flexibility to handle the different requirements for a comprehensive range of use cases.

Figure 2-4 shows four 5G use case segments proposed for the evolution of Cellular IoT.

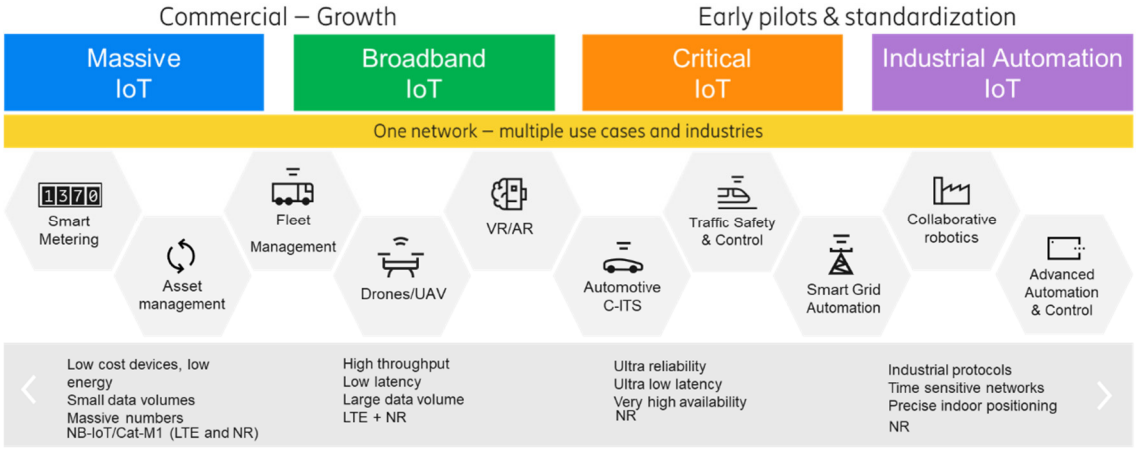

Figure 2-4 5G use cases segments proposed for the evolution of Cellular IoT

The **Massive IoT** segment supports very low-cost devices with long battery life, deployed in massive numbers and supporting use cases that demand very low data usage in the networks – use cases such as fleet management or logistics, asset management or smart metering. This segment is already deployed in today's Long-Term Evolution (LTE) commercial networks and is continuing to grow in terms of ecosystem and numbers of connections.

3GPP standardised three new technologies for massive Machine Type Communications (MTC) in Release 13: Extended Coverage GSM IoT (EC-GSM-IoT), LTE-M and NB-IoT. LTE-M extends LTE with new features for improved battery life, extended coverage and support for low-complexity device category series, named Category M (CAT-M). NB-IoT is a standalone radio access technology based on LTE that enables extreme coverage and extended battery lives for ultra-low complexity devices.

LTE-M and NB-IoT should target complimentary use cases. LTE-M is better suited for applications that require higher throughput, lower latency, better positioning and voice connections. Typical LTE-M use cases include wearables, sensors, trackers, alarm panels and customer support buttons, all with support for data and voice connections. On the other hand, NB-IoT is the technology of choice for very low throughput applications that are tolerant of delay but require very good coverage, such as simple utility meters and sensors deployed in challenging radio conditions.

The **Broadband IoT** segment uses the capabilities of Mobile BroadBand (MBB) to achieve higher throughput, low latency and larger data volumes than Massive IoT can support and together with some additional functionality can support IoT use cases for drones or Unmanned Aerial Vehicles, Augmented Reality and Automotive. This segment can already be supported in today's 4G network and will be able to support even more advanced use cases when moving from 4G to 5G with the higher speed, lower latency and other capabilities that 5G will bring.

The **Critical IoT** enables extremely low latencies and ultra-high reliability at a variety of data rates. This segment addresses extreme connectivity requirements of many advanced wide area and local area applications in intelligent transportation systems, smart utilities, remote healthcare, smart manufacturing and fully immersive Augmented Reality/Virtual Reality. Powered by the most innovative capabilities of 5G NR, Critical IoT is expected to enable many new use cases within the IoT arena.

For the most complex segment, the **Industrial Automation** segment, some very challenging use cases specific to the industrial campus and manufacturing environments can be supported – use cases such as collaborative robotics which would require functionality such as industrial protocols in addition to time sensitive networks and very precise positioning.

1.9 Device availability

Figure 2-5 shows the approximate timing of 5G device availability [3]. Early Fixed Wireless Access (FWA) devices have been developed to meet market needs in the USA and Australia for example. The first 3GPP-compliant 5G smartphones and tablets are likely to be launched in 2019. To date, the IoT business has primarily been driven by the affordability of devices. Costs of 3GPP-compliant devices have come down significantly recently, and as they approach 5–10 euros, we are starting to see the cellular-delivered IoT market becoming better established. The market for industrial IoT, or critical machine to machine communications, services is at an earlier stage, but will likely be a significant market in the longer term. We foresee 3GPP systems becoming the IoT technologies of choice for operators and industry in the longer term.

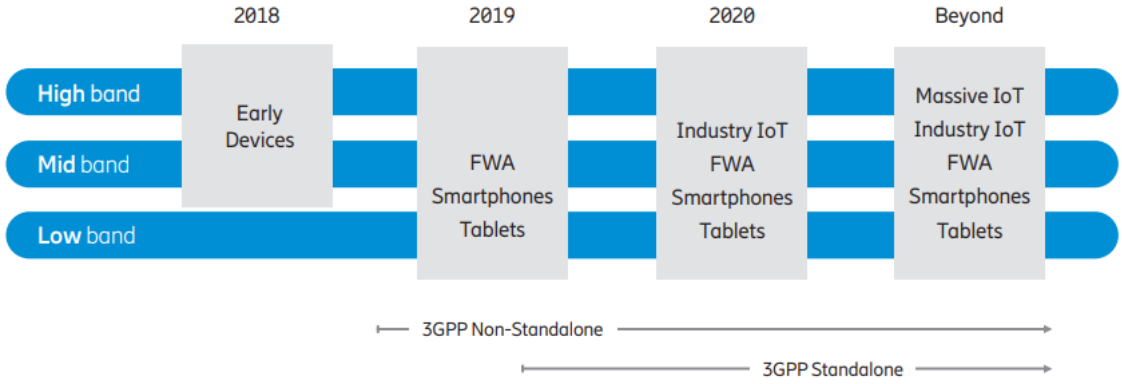

Figure 2-5 5G device availability

1.10 The global spectrum picture

Figure 2-6 gives a general indication of spectrum availability across all mobile network generations over time [3]. The spectrum available to 5G will vary from market to market, according to whether it is already in use and the timing of auctions and licensing processes.

More spectrum will be needed for 5G, because its benefits are fully achieved in new millimeter wave frequencies, with extremely wide bands. Here, the ultra-high peak rates and low latency are most likely to be used to add new levels of capacity and throughput for enhanced mobile broadband, especially as a way of offloading congested 4G networks (and for new special use cases). But there is also broad interest in deploying 5G technology in new mid bands (3.5–6GHz) and existing, legacy mid bands (1.8–2.6GHz) as a way of achieving national 5G coverage as rapidly as possible.

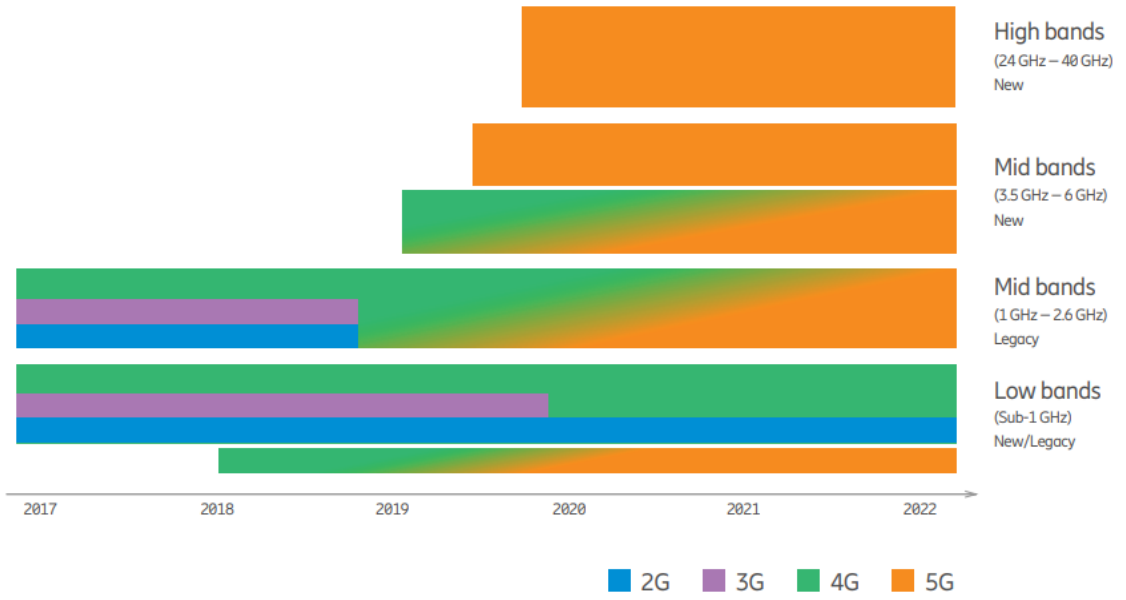

Figure 2-6 Spectrum allocation over time

Each spectrum band has different physical properties, meaning there are trade-offs between capacity, coverage and latency, as well as reliability and spectral efficiency, as illustrated in Figure 2-7. If the network is optimised for one metric, there may be degradation of another metric.

Low-band spectrum has historically been used in 2G, 3G and 4G networks for voice and mobile broadband services, as well as broadcast TV. The available bandwidth is typically between 10MHz and 30MHz. This makes this spectrum most suitable for wide-area and outside-in coverage from macro base stations. For a typical 5G mobile broadband use case, capacity and latency are similar to 4G on the same band.

Legacy mid-band spectrum is currently used for 2G, 3G and 4G services. New mid-band spectrum has typically been allocated in 3.5GHz spectrum bands. In these bands, especially in the new higher spectrum, we are likely to see larger bandwidths (50–100MHz). This will enable high-capacity, lower latency networks which can be used for new 5G use cases, with better wide-area and indoor coverage than higher-band spectrum.

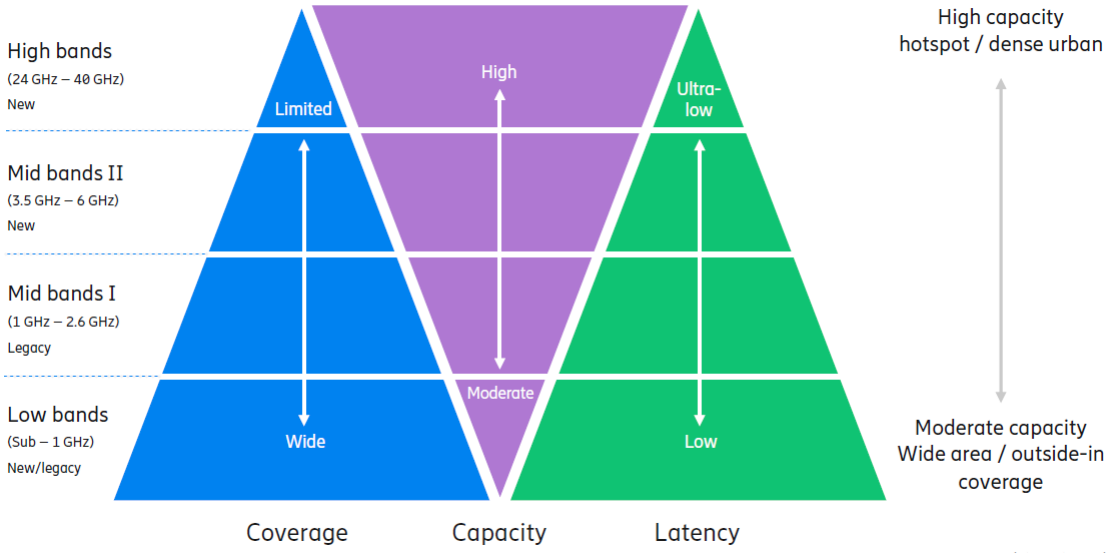

Figure 2-7 Spectrum trade-off

High-band spectrum provides the quantum leap in performance promised by 5G. These new spectrum bands are typically in the 24–40GHz range, with bandwidths in 100MHz (or larger) blocks. Such large bandwidth enables ultra-high spectrum capacity networks (5–10 times higher than today), with latency as low as 1ms. However, these higher frequencies come with a coverage limitation compared with lower bands.

1.11 Two-phase approach

As 5G will need to coexist and interwork with 4G for many years to come, we are likely to see the vast majority of these deployments as non-stand-alone (NSA) initially, as a way of reducing time to market and ensuring good coverage and mobility. The 5G stand-alone (SA) mode, which requires a new (service-based) core network architecture (known as 5G Core, or 5GC), will enable deployments of 5G as an overlay to, or independent, of 4G coverage.

To achieve nationwide coverage as fast as possible, we're also likely to see 5G deployed in low/mid bands, which will also be suitable for massive IoT use cases in the future. SA 5G in high bands is more likely to be used mainly for data offload in high-traffic areas, as separate networks in factories or campuses, and for critical IoT in data-intensive applications.

Ericsson favors a two-phase approach to deploying 5G as shown in Figure 2-8. 3GPP standardised options shown in the figure will be followed. In the phase 1 (left half of the figure), enhanced MBB is supported and Low Latency IoT use cases will be supported during 2019/2020. This is referred to as 5G NSA mode. In the phase 2 (right half of the figure), 5G network will operate in SA mode, with both control and user planes carried over 5G NR access.

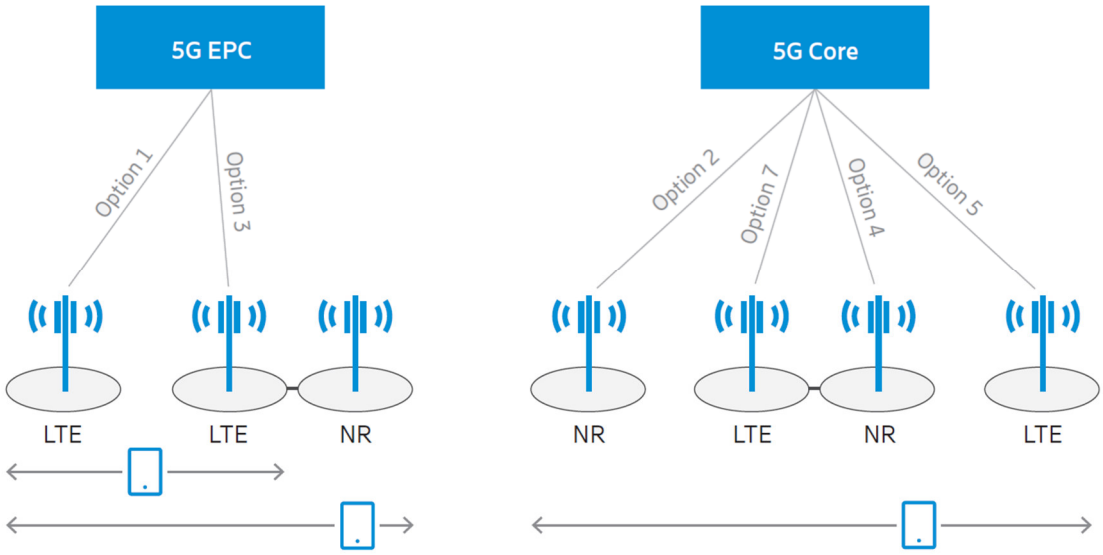

Figure 2-8 LTE-NR connectivity options towards 5G Evolved Packet Core and 5G Core

1.12 Network slicing

The technique of network slicing allows for the definition of multiple logical networks (or slices) on top of the same physical infrastructure. Resources can be dedicated exclusively to a single slice or shared between different slices.

The technique of Network Slicing allows for the definition of multiple logical networks (or slices) on top of the same physical infrastructure Figure 2-9 [7]. Resources can be dedicated exclusively to a single slice or shared between different slices.

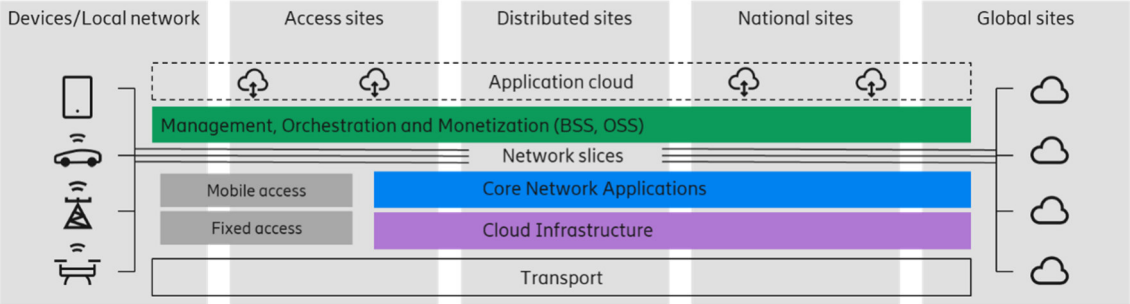

Figure 2-9: 5G Network Slicing

A network slice is built to address a desired behaviour from the network. Such behaviour can be associated with security, data-flow isolation, quality of service, reliability, independent charging and so on. A network slice may support one or several services and can be used to create a virtual operator network and may provide customised service characteristics. Network slicing can be used for several purposes: a complete private network, a copy of a public network to test a new service, or a dedicated network for a specific service.

For instance, when setting up a private network in the form of a network slice that can be an end-to-end virtually isolated part of the public network, the network exposes a set of capabilities in terms of bandwidth, latency, availability and so on. Thereafter, a newly created slice can be locally managed by the slice owner who will perceive the network slice as its own network complete with transport nodes, processing and storage. The resources allocated to a slice can be a mix of centrally located and distributed resources. The slice owner can initiate applications from its management center, and applications will simply execute and store data, either centrally, in a distributed management system or a combination of both.

1.13 Distributed Cloud

As shown in Figure 2-10, Ericsson defines the **Distributed Cloud** [8] as a cloud execution environment that is geographically distributed across multiple sites, including the required connectivity in between, managed as one entity and perceived as such by applications. The key characteristic of our distributed cloud is abstraction of cloud infrastructure resources, where the complexity of resource allocation is hidden to a user or application. Our distributed cloud solution is based on Software Defined Networking (SDN), Network Functions Virtualization (NFV) and 3GPP edge computing technologies to enable multi-access and multi-cloud capabilities and unlock networks to provide an open platform for application innovations.

Ericsson Distributed Cloud solution enables edge computing, which many applications require. It defines **Edge Computing** as the ability to provide execution resources (specifically compute and storage) with adequate connectivity at close proximity to the data sources.

The distributed cloud relies on efficient **management and orchestration** capabilities that enable automated application deployment in heterogeneous clouds supplied by multiple actors. Figure 2 9 illustrates how the service and resource orchestration spans across distributed and technologically heterogeneous clouds. It enables service creation and instantiation in cloud environments provided by multiple partners and suppliers. When deploying an application or a Virtual Network Function (VNF), the placement decisions can be based on multiple criteria, where latency, geolocation, throughput and cost are a few examples. These criteria can be defined either by an application developer and/or a distributed cloud infrastructure provider, serving as input to the placement algorithm.

Each of the layers in the distributed cloud stack will expose its capabilities. The cloud infrastructure layer and the connectivity layer will expose their respective capabilities through the **Application Programming Interface(s)** (API(s)), which will then be used by application developers of the industries making use of the mobile connectivity. By setting developer needs in focus, the exposed API(s) will be abstracted so that they are easy to use.

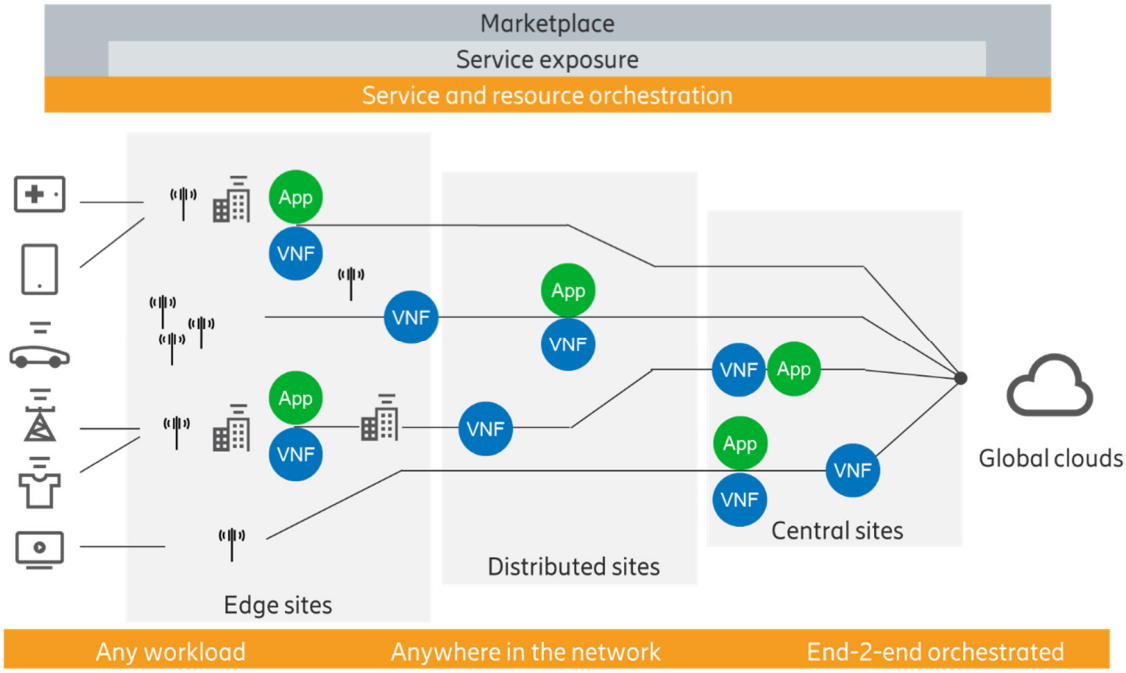

Figure 2-10 Distributed cloud architecture

1.13.1 Edge Cloud Computing concept

What is Edge Computing? Edge Computing places high-performance compute, storage and network resources as close as possible to end users and devices [5]. Doing so lowers the cost of data transport, ecreases latency, and increases locality. Edge Computing will take a big portion of today's centralised data centers and cloud and put it in everybody's backyard.

Edge Computing can be split into two layers: Device Edge and Infrastructure Edge layer. Infrastructure edge can be further split into two sublayers: Access Edge and Aggregation Edge sublayer.

Device Edge

The Device Edge refers to edge computing resources on the device side of the last mile network. Some devices will be single function, such as embedded sensors, designed to perform very specific tasks and deliver streams of data to the network. Other edge devices will act as specialized gateways, aggregating and analysing data and providing some control functions. And yet other edge devices will be fully-programmable compute nodes, capable of running complex applications in containers, virtual machines, or on bare metal. The Device Edge will be the basis of many useful applications which require the lowest possible latency, as device edge resources are as close as it is possible to be to the end user.

However, it is already clear that many device edge resources will be connected to the cloud and be managed as extensions of the cloud. They will largely be connected to the Infrastructure Edge (IT resources which are positioned on the network operator or service provider side of the last mile network) over wired and wireless networks and that workloads running on the Device Edge will be coordinated with workloads running on the Infrastructure Edge. In many cases it will be both more reliable and less expensive to run workloads on the Infrastructure Edge rather than entirely on the edge devices.

Access Edge

The Access Edge is the part of the Infrastructure Edge closest to the end user and their devices. Edge data centers deployed at or very near to the Access Edge are typically directly connected to a radio or other front-line network infrastructure, and they are used to operate application workloads for complex tasks such as machine vision and automated decision support for large-scale IoT. Edge data centers deployed at the Access Edge, a sublayer within the Infrastructure

Edge, may also connect to other edge data centers which are deployed above them in a hierarchical architecture at the Aggregation Edge sublayer.

Aggregation Edge

The Aggregation Edge refers to a second sublayer within the Infrastructure Edge which functions as a point of aggregation for multiple edge data centers deployed at the Access Edge sublayer. The purpose of this layer is to provide a reduced number of contact points to and from other entities, such as a centralized cloud data center and the Infrastructure Edge and to facilitate the collaborative processing of data from multiple Access Edge sublayer edge data centers. The Aggregation Edge is typically two network hops from its intended users but is still much closer to them than the centralized cloud data center, and it is thus able to achieve far lower latencies.

Cloud interoperation

Figure 2-11 shows Edge Computing layers and its relation to the central cloud. It is important to notice that the Edge Computing does not exist by itself. Despite the level of computing power and performance that is achievable between the combination of the Device Edge and Infrastructure Edge, both of these entities benefit immensely from tight, cohesive interoperation with the centralised cloud.

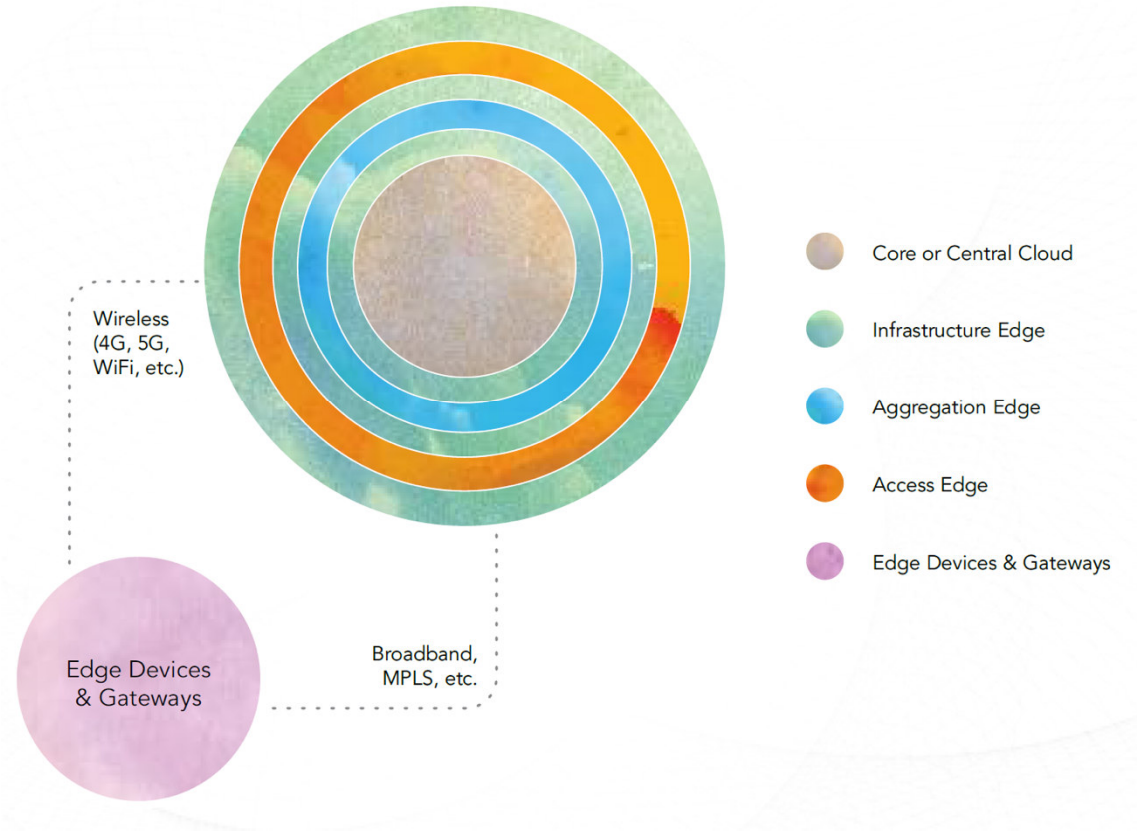

Figure 2-11 Edge cloud layers

As can be seen in Figure 2-11, both the Device and Infrastructure edge can be viewed as complementary to, and even as extensions of, the existing centralised cloud. By connecting these distributed resources together and creating an Edge Cloud which spans from the current centralised data center, through the Infrastructure Edge and its sublayers through to the Device Edge, the cloud operator will be able to dynamically allocate resources and direct voltage management application workloads to the optimal location for them, regardless of whether that is in the Device Edge, Infrastructure Edge or the centralised cloud. For the optimal deployment of the voltage management applications, power grid characteristics, e.g., number of nodes, meshed grid, density, area spanned by a Distribution System Operator (DSO), will have to be taken into consideration. The following sections elaborate on this topic.

Edge-native applications, as their name suggests, are applications which require the unique characteristics provided by edge computing to function satisfactorily, or in some cases to function at all. These applications will typically rely on the low latency, locality information or reduced cost of data transport that edge computing provides in comparison to the centralised cloud. Voltage management applications were built as edge-native applications in RESERVE project. For further details, please see Chapter 3.

1.13.2 Cloud Radio Access Network

Cloud Radio Access Network (C-RAN) is a novel mobile network architecture which can address a number of challenges that mobile operators face while trying to support ever-growing end-users' needs towards 5th generation of mobile networks (5G) [6]. The main idea behind C-RAN is to split the base stations into radio and baseband parts [1], and pool the BaseBand Units (BBUs) from multiple base stations into a centralised and virtualised BBU Pool, while leaving the Remote Radio Heads (RRHs) and antennas at the cell sites. This gives a number of benefits in terms of cost and capacity.

C-RAN architecture is targeted by mobile network operators, as envisioned by China Mobile Research Institute, IBM, Alcatel-Lucent, Huawei, ZTE, Nokia Siemens Networks, Intel and Texas Instruments. Moreover, C-RAN is seen as a typical realization of mobile network supporting soft and green technologies in fifth generation (5G) mobile networks.

Figure 2-12 shows an example of a C-RAN mobile LTE network. The fronthaul part of the network spans from the RRHs sites to the BBU Pool. The backhaul connects the BBU Pool with the mobile core network. At a remote site, RRHs are co-located with the antennas. RRHs are connected to the high-performance processors in the BBU Pool through low latency, high bandwidth optical transport links.

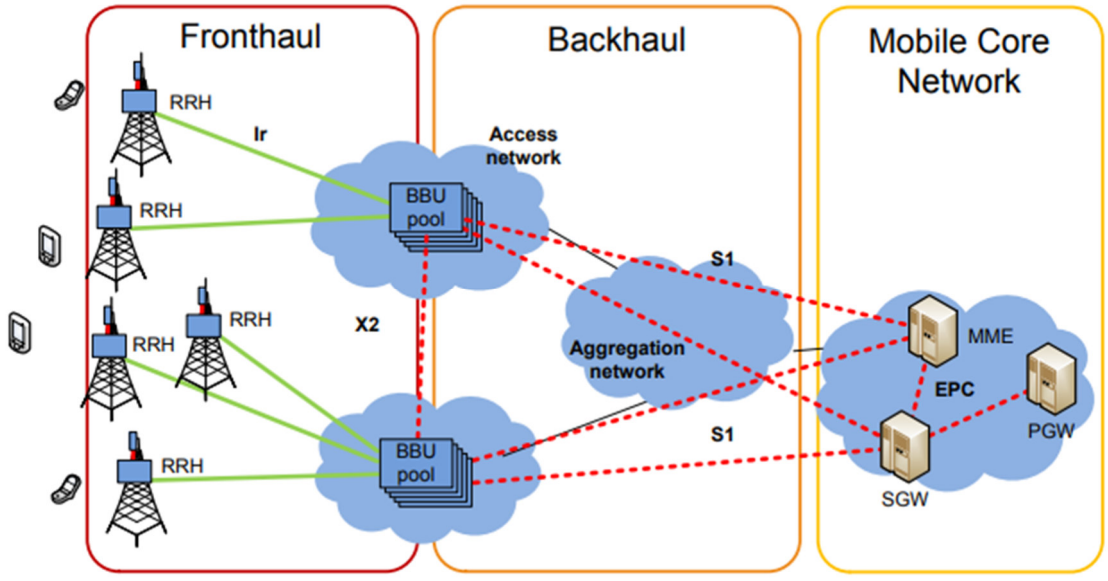

Figure 2-12 C-RAN LTE mobile network

[1] Baseband refers to the original frequency range of a transmission signal before it is converted, or modulated, to a different frequency range. For example, an audio signal may have a baseband range from 20 to 20,000 hertz. When it is transmitted on a radio frequency (RF), it is modulated to a much higher, inaudible, frequency range.

1.14 5G security

Connected devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy, and the 5G system is designed with these requirements in mind [4]. Figure 2-13 shows five core properties that contribute to the trustworthiness of the 5G system: resilience, communication security, identity management, privacy and security assurance. These properties of the 5G system contribute toward creating a trustworthy communications platform that is an ideal foundation on which to build large-scale, security-sensitive systems, including those used in industrial settings.

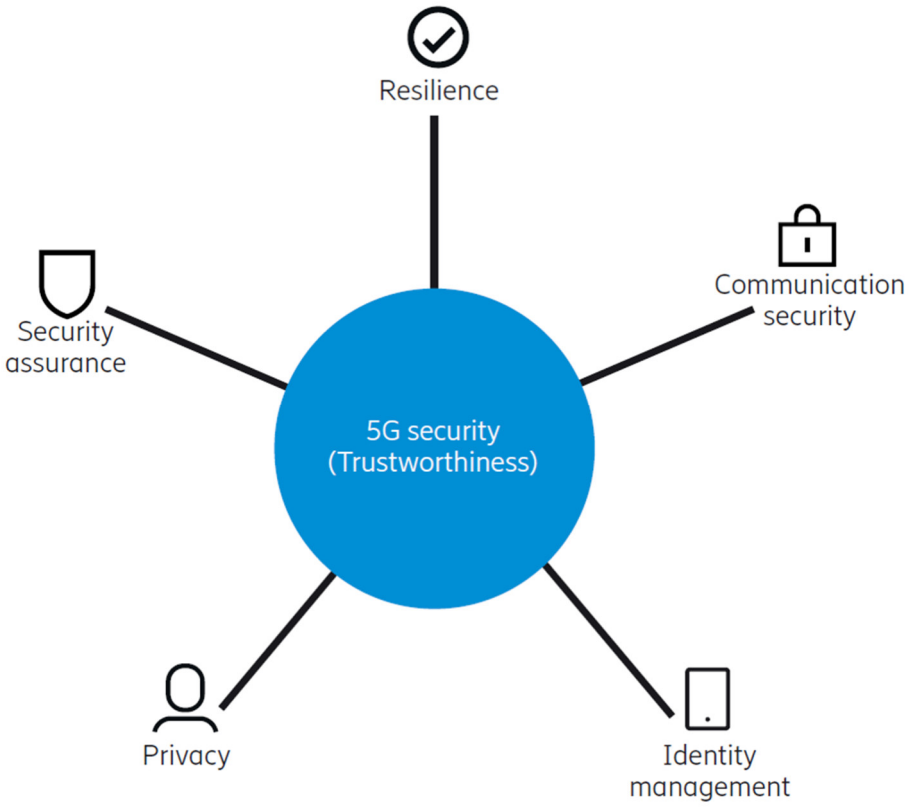

Figure 2-13 Five properties that contribute to the trustworthiness of the 5G system

Resilience

The 5G system's resilience to cyberattacks and non-malicious incidents comes through a variety of complementary and partially overlapping features. First, the 5G NR access was developed for Ultra-Reliable Low Latency Communications (URLLC). Even greater resilience against failures and attacks can be obtained by deploying a single base station as two split units, called a central unit and a distributed unit. This split also facilitates customizable deployment of security sensitive functions of the 5G NR access, such as user plane encryption, in a secure central location while keeping non-security sensitive functions in less secure distributed locations. Next, the 5G core network architecture itself is designed around resilience concepts. For example, network slicing isolates groups of network functions from other functions. Service Based Architecture principles are another architectural concept that enhances resilience. These principles make use of software and cloud-based technologies that improve on the more static and node-centric designs of previous generation networks. The resilience of the 5G system also stems from the strong mobility support that it shares with previous generation 3GPP networks, which ensures continuous secure connectivity for devices moving from one location to another. In addition to these general features providing resilience, there are more specialised functions introduced to operate a radio access network in extreme situations, such as when it has become separated from its core network. This is called isolated Evolved UMTS (Universal Mobile Telecommunication System) Terrestrial Radio Access Network (E-UTRAN) operation for public safety in 4G/5G and is very useful in disaster areas, for example. Finally, partly due to strong

regulations and associated high fines, cellular networks have long adhered to high carrier-grade availability requirements.

Communication security

The 5G system provides secure communication for devices and for its own infrastructure. In particular, the new Service Based Architecture (SBA) for core network communication takes threats from the interconnect network into account. The 5G system includes protection against eavesdropping and modification attacks. Signalling and user plane traffic is encrypted and can be integrity protected. The strong and well-proven security algorithms from the 4G system are reused. These are encryption algorithms based on SNOW 3G (word-based synchronous stream cipher with name SNOW) [10], Advanced Encryption Standard Counter (AES-CTR) [11], and ZUC (Cryptographic algorithm with name ZUC) [9]; and integrity algorithms based on SNOW 3G, Advanced Encryption Standard Cipher-based Message Authentication Code (AES-CMAC) [12], and ZUC. The main key derivation function is based on the secure Hash-based Message Authentication Code Secure Hashing Algorithm 256-Bits (HMAC-SHA-256) [13]. Mobility in the 5G system also inherits different security features from the 4G system.

Identity management

At its heart, the 5G system has secure identity management for identifying and authenticating subscribers, roaming or not, ensuring that only the genuine subscribers can access network services. It builds on strong cryptographic primitives and security characteristics that already exist in the 4G system. One of the most valuable new security features in the 5G system is the new authentication framework where mobile operators can flexibly choose authentication credentials, identifier formats and authentication methods for subscribers and IoT devices. Previous mobile network generations required physical Subscriber Identity Module (SIM) cards for credentials, but the 5G system also allows other types of credentials such as certificates, pre-shared keys and token cards. Another valuable new security feature is the ability of a subscriber's operator to determine the presence of the subscriber during an authentication procedure – even when roaming. The 5G system also inherits a mechanism from legacy systems, called Equipment Identity Register (EIR) check, which can be used to prevent stolen devices from using the network services, thereby discouraging device theft.

Privacy

Data traffic, including phone calls, internet traffic and text messages, is protected using state-of-the-art encryption. The devices and the network mutually authenticate each other and use integrity-protected signalling. Another privacy enhancement is protection of subscriber identifiers, both long-term and temporary, e.g., subscriber's long-term identifier concealment mechanism that is based on the Elliptic Curve Integrated Encryption Scheme (ECIES) [14]. In addition, the 5G system enforces a stricter policy for update of temporary identifiers. Further, the 5G system is also able to detect false base stations that are the root cause of International Mobile Subscriber Identity (IMSI) or Temporary Mobile Subscriber Identity (TMSI) catchers.

Security assurance

In 3GPP, security assurance is a means to ensure that network equipment meets security requirements and is implemented following secure development and product lifecycle processes. This assurance is especially important for mobile systems, as they form the backbone of the connected society and are even classified as critical infrastructure in some jurisdictions. 3GPP and Global System for Mobile communications Association (GSMA) took the initiative to create a security assurance scheme called the Network Equipment Security Assurance Scheme (NESAS) [15], which is suitable to the telecom equipment lifecycle. NESAS comprises two main components: security requirements and an auditing infrastructure. The security requirements defined on node basis and collected in so-called SeCurity Assurance Specifications (SCAS) are defined jointly by operators and vendors in 3GPP. The auditing infrastructure is governed by the GSMA, the global mobile operator organization, that conduct the audits of vendors' development and testing processes.

1.15 5G public and private networks

New 5G deployment architectures options are being investigated considering public and non-public network deployment options for verticals such as manufacturing [16]. In the coming

years, 5G will enable many new industrial automation applications using public and non-publicly operated 5G networks. Private networks can be deployed as isolated, standalone networks and in conjunction with a public network. In certain deployments of a private network in conjunction with a public network, private and public networks can share part of a radio access network. 3GPP specifications include functionality that enables RAN sharing [17].

3. Scenarios and ICT Requirements

1.16 Scenarios for Active Voltage Management

1.16.1 Energy system requirements

The output of the Active Voltage Management (AVM) algorithm, a Volt-VAr curve (VVC), is the deployable element of the AVM from a trial site perspective. Key to the execution of the VVC is the availability of device readings for the inverter at each trial site and the availability to send back down control messages. To achieve this there were three architectures identified **Centralised**, **Decentralised** and **Hybrid-Edge Computing**. All three of these potential architectures have been found to be perfectly viable and can be used to address the deployment and/or execution of the Volt-VAr curve at the target RES device. It is worth mentioning that in all three solutions the Volt-VAr curve has been generated offline and is then sent via ICT to the point of execution in a different way for each solution. Note that the generation of the Volt-Var is outside the scope of the analysis of the three solutions from an ICT perspective. The choice of ICT architecture is driven by certain features relevant to each trial site and these features, among others, are level of access to the RES device, network connectivity at the physical location, inverter capability and RES device saturation at the physical location.

Table 3-1 presents the minimum high-level ICT requirements needed to effectively run the AVM and it is those requirements that the following assessments of each trial site are compared against. These requirements were gathered and defined as part of activities in WP1 that examined the implementation of the AVM from a power systems perspective.

Table 3-1: ICT Aspects of Active Voltage Management

ICT Aspect	Active Voltage Management Minimum Requirements
Latency per Cycle	2 to 4 seconds Limited number of messages, algorithm is executed on local edge level
Typical Message Size	Up to 100KB (updating the Volt-Var properties)
Acceptable Packet Loss	None (use protocol with retransmissions)
Availability Unplanned downtime	99.99% Below 4.38 minutes per month
Resilience	Incomplete or distorted messages must be checked and re-transmitted
Data Security	Maximum protection against any form of illegal intrusion into the communications system, including reading, changing or deleting data during transmissions or in storage
Privacy	Must meet all applicable national and European regulations

The following sections contain a presentation of these results, a comparison of those results with those detailed Table 3-1. This section will conclude with a set of recommendations based on the findings with a set of use cases. These use cases will detail criteria in which each solution could be applied and also some of the solution specific steps needed to optimise the implementation.

Centralised Volt-Var Curve Execution

Table 3-1 above is a summary of our findings for the ICT performance of the centralised architecture. From a latency perspective this method is the most susceptible to delay as it is dependent on the readings being sent over the network and the set point being sent back to the RES inverter. In Table 3-1, a 2 to 4 second delay per cycle was detailed as being acceptable and

as seen in Table 3-2 this the latency measured over one week was between 110 and 1095 milliseconds. It also must be noted that security in the centralised implementation of the AVM was critical, so it was decided to password protect access to the connection endpoints and also Transport Layer Security (TLS) encrypt all traffic. All other criteria as laid out in, were met and in some cases exceeded.

Table 3-2: ICT communications assessments for the Centralised architecture

ICT Aspect	Centralised Volt-Var Curve Execution
Req-AVM-endPoints	In centralised Volt-Var Curve (VVC) scenario, bidirectional communication will take place between central cloud controller and RES units. Up to 10,000 RES units can be connected to the central controller with a wide geographical spread, potentially 200km between devices.
Req-AVM-latency	110 – 1,095ms varying on network connectivity and site network load
Req-AVM-sampleRate	Every 5 seconds
Req-AVM-volume	75 – 80 Bytes
Req-AVM-reliability	Availability/unplanned downtime is 99.99% (below 4.38 minutes per month). Incomplete or distorted messages must be checked and re-transmitted.
Req-AVM-security	All communications between AVM execution cloud controller and the trial site cloud platform are password protected and TLS v1.2 secured to ensure maximum protection against any form of illegal intrusion into the communications system, including reading, changing or deleting data during transmissions or in storage.

The ICT parameter End-Points indicates a number of communications end-points. Those are usually measurement devices connected to the energy network that send measured values to the control point and receive the control signal from the control point.

The Latency parameter indicates the transmission time for a measurement or control signal to be sent from point A to point B over the communications network.

The Sampling Rate shows how frequently measurements need to be transmitted between the device and the control center (or vice versa).

The Data Volume is the maximum size of a standard message transmitted between end-points, including overhead for addressing, time stamps, authentication and authorisation, encryption, et al.

Reliability indicates the requested ability of communications where messages are guaranteed to reach their destination complete and uncorrupted and in the order they were sent.

Security indicates the requested ability to prevent an unauthorised access to telecommunications traffic, or to any written information that is transmitted or transferred.

Decentralised Volt-Var Curve Execution

Given that the decentralised approach is less network dependant, with the AVM execution taking place on the RES inverter, the ICT criteria around latency and message size are less relevant. In a security context, the same steps are applied in terms of cyber security and access but with added consideration to secure any supplemental hardware devices required to enhance the capabilities of the existing hardware to enable the execution of the AVM. All other criteria as laid out in Table 3-1, were met and in some cases exceeded.

Table 3-3: ICT communications assessments for the Decentralised architecture

ICT Aspect	Decentralised Volt-Var Curve Execution

Req-AVM-endPoints	In the decentralised implementation the AVM is executed on the device, therefore one endpoint per implementation would describe the amount of endpoints.
Req-AVM-latency	<110ms
Req-AVM-sampleRate	Every 10 seconds
Req-AVM-volume	75 – 80 Bytes
Req-AVM-reliability	Availability/unplanned downtime is 99.99% (below 4.38 minutes per month). Incomplete or distorted messages must be checked and re-transmitted.
Req-AVM-security	As the AVM execution takes place on the inverter or a device connected directly to the inverter the security aspect is more physical but any communications by way of monitoring and VVC update will be TLSv1.2 secured to ensure that the threat of illegal intrusion from a communications perspective is negated.

Hybrid Edge Computing Volt-Var Curve Execution

Given that this execution contains a combination of the network dependant centralised implementation over shorter distances and the decentralised implementation of the same ICT criteria. At present, there is no implementation deployed in the field but in all aspects, apart from latency, the assessment results will be a combination of those gathered from the decentralised and centralised implementations. From a latency perspective, given that the distances between the connected endpoints detailed in the description of the Hybrid Edge Computing VVC execution in A.1.3, the latency will be lower than that of the centralised implementation.

Table 3-4: ICT communications assessments for the Hybrid architecture

ICT Aspect	Hybrid Volt-Var Curve Execution
Req-AVM-endPoints	In hybrid VVC scenario, bidirectional communication will take place between distributed edge application and RES units. Up to 100s of RES units can be connected to a single node with multiple nodes managed by a single central controller. The distance between devices connected to each node would be envisaged as being <20km with the central control distance from each node being around 200km.
Req-AVM-latency	<1000ms varying on network connectivity and site network load
Req-AVM-sampleRate	Every 5 seconds
Req-AVM-volume	75 – 80 Bytes
Req-AVM-reliability	Availability/unplanned downtime is 99.99% (below 2 minutes per month). Incomplete or distorted messages must be checked and re-transmitted.
Req-AVM-security	As the AVM execution takes place on the inverter or a device connected directly to the inverter the security aspect is more physical but any communications by way of monitoring and VVC update will be TLSv1.2 secured to ensure that the threat of illegal intrusion from a communications perspective is negated.

1.16.2 Timescales and preconditions relevant to the commercial scale use of Active Voltage Management

Validation of the AVM scenarios is ongoing. The improvement is needed to make the implementation efficient. Tuning and improvement of the AVM mechanism is being worked on at

the moment by the project partners. Accordingly, the AVM implementation in commercial networks could be done now.

In the AVM scenarios, communications are needed but the communication requirements are not challenging. In the current implementation the AVM algorithms are running on standard scalable IT platforms (Microsoft Azure and Kubernetes). In order to provide the commercial solution, the dashboard needs to be prepared and further system adaptations need to be done. While the communications requirements are not challenging, interoperability in terms of interfacing with the physical devices would add a level of financial cost per installation, as in some cases the hardware deployments were required to allow the AVM to operate. However, some of these costs could be lessened or even negated if standards were developed that would define the ICT interfaces, both in hardware and software, that should be provided so that solutions like AVM could be used.

1.16.3 ICT solutions

During the course of the deployment and testing of the AVM, careful consideration was paid to the reasons for choosing an architecture suitable for each deployment. These reasons are based upon the semantics of the deployment location and the ICT requirements of each solution. The following scenarios detail a deployment location and how an execution architecture of the AVM system would be applicable to each scenario.

1.16.3.1 Scenario 1 - Aggregator Controlled Inverters

In modern grid systems the presence of Aggregators and their control of the RES devices via bespoke Distributed Energy Resource Management Systems (DERMSs) is becoming more common. This is acting as a type of firewall in terms of control of the device from a centrally controlled grid system that looks to ensure the stability of the overall network from a voltage perspective by deploying algorithms like AVM across the grid. To overcome this, cooperation from both the aggregator and the grid operator is required and it is necessary that both systems communicate to ensure that the AVM gets deployed and voltage stability is maintained. In this case, more often than not in modern systems, this communication will be cloud-to-cloud and a **centralised architecture** for the AVM execution would be most applicable. This architecture would afford the aggregator with a layer of data agnostics with only the values applicable to the AVM execution being sent to the system operator for the generation of the reactive power set-point. Given that very low latency is not a high priority requirement for AVM and that the packet size and message frequency is low, core to the ICT deployment is the security of the communication and privacy with how the data is treated. Security and privacy are key and the responsibility for this is on both parties. While the deployment of the AVM for this scenario could be carried out using both the Hybrid-Edge or Decentralised architectures, the centralised architecture is less invasive and is less dependent on the hardware and software capabilities at the edge due to the already integrated aggregator owned DERMS control system being used.

5G aspects

The following ICT solutions for Scenario 1 that are common for several other scenarios are listed here and described in detail in Chapter 4:

- Providing communications links to new end-points in the energy system
- Use of communications friendly protocols to maximise the reliability of the communications
- Network Slicing for energy provider control of QoS and security features
- Use of public 5G networks without network slicing and public 4G LTE networks
    - Mobile networks for massive IoT communications

1.16.3.2 Scenario 2 - Remote Communications Constrained RES Device

With the Distributed Energy Resource deployment becoming common and with the potential of some of these units being deployed to geographical regions with limited network connectivity comes the need for the control mechanisms, like AVM, to be deployed in a way that is not dependant on having a full-time dedicated communications link. This would mean that any deployment, as far as possible, should be stand alone and the most applicable architecture for this would be the **decentralised architecture** detailed in A.1.1. This method of deployment would rely heavily on the hardware and software capabilities of the inverter for AVM deployment but from an ICT perspective it would only require communications to send the VVC to the inverter and if the VVC were changed to update it on the inverter. The inverter capability is a key factor

for this deployment as the inverter will either require functionality to receive the VVC and execute it as in the case of the Solar PhotoVoltaic (PV) deployment detailed in D5.2 or have interfacing capabilities with a supplementary piece of hardware that can run the AVM execution program and send the control messages to the device as is the case with the Vehicle-to-Grid (V2G) implementation detailed in D5.2. Latency, frequency and message size are not an issue in the deployment of this architecture as all the data needed is either on or beside the inverter. Protection and device access either in a physical or virtual way must be ensured to maintain the integrity of this deployment but from the perspective of network security and privacy the scope for attack is very narrow due to minimal external data transfer and communications. While the centralised solution may not be viable for this deployment due to network connectivity issues, the Hybrid-Edge computing solution may be viable if there were a large proliferation of Distributed Energy Resources (DER) in the area as it may be then cost effective to provide a dedicated communications base station on site with a centrally held database of VVCs specific to each DER at the location.

5G aspects

As this scenario has undemanding requirements for the communications, any communication infrastructure could be used.

1.16.3.3 Scenario 3 - DER Cluster Control

In urban areas the scope to deploy DER is increasing with battery storage and rooftop solar PV becoming more common and easier integrate into the power grid. This scenario is centred around providing voltage stability to an urban area where there is a high saturation of DER. The issue to be addressed with this scenario would be that the DERs connected to the grid may be owned by different entities and may have different software and hardware capabilities but given that their proximity may be close their combination may impact negatively on stability, thus viewing, analysing and controlling these as one entity may be required. To achieve this using a centralised architecture would require a great degree of complexity and would involve a large volume of network traffic potentially travelling over large distances. While a decentralised approach would be an option it would require frequent updating of the VVC at each DER due to the saturation of instable RES sources causing a real time lack of system awareness thus this approach would not provide an adequate level of dynamism to cater for the complexity of the system. Therefore, the most suitable solution would be the **Hybrid-Edge Computing architecture**. It would add a layer of control between the central controller and the DER to hand off the system awareness at a granular level to software hosted at communications base stations. This secondary layer would handle the control of DERs in its immediate geographical region whether this control be the direct propagation of the VVC to the inverter or the receipt of readings from the RES device and the execution of the AVM algorithm at the base station with the reactive power setpoint being returned. This method of deployment of the AVM is heavily reliant on robust and available communications on the base station to ensure that voltage stability can be maintained across the cluster in unison and security at this point is also key due the impact of a malicious attack at a secondary control would be service effecting.

5G aspects

While mobile-edge cloud computing is a new paradigm to provide cloud computing capabilities at the edge of pervasive radio access networks in close proximity to mobile users [2], and is a key feature of 5G, it may be unrealistic to assume that the edge cloud will be collocated to every radio base station in the network, which will be prohibitive due to high costs. Ericsson is providing a Radio Access Network (RAN) Cloud solution that could be used in this scenario and could even be used in the first scenario with centralised architecture. In this RAN Cloud solution, the edge cloud is centralising radio access functions, which means the edge cloud can cover the area with typical diameter of 50km. In such big urban coverage up to 50 SSAUs can be located connecting up to 25,000 RES devices.

This scenario 3 solution should take into consideration that this area will be served by multiple DSOs. Each DSO may have its own Active Voltage Management solution, or they may use the same solution. The DSO would be granted dedicated cloud resources within the edge cloud. This would mean that the overall regional Active Voltage Management instance could be deployed in the same edge cloud that could coordinate multiple DSO instances if needed.

In addition, the following ICT solutions for Scenario 3 that are common for several other scenarios are listed here and described in detail in Chapter 4:

- Providing communications links to new end-points in the energy system
- Use of communications friendly protocols to maximise the reliability of the communications
- Network Slicing for energy provider control of QoS and security features
- Use of public 5G networks without network slicing and public 4G LTE networks
- Using Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms
- Use of private 4G or 5G networks
- Mobile networks for massive IoT communications

1.17 Scenarios for Dynamic Voltage Stability Monitoring

1.17.1 Energy system requirements

When the share of renewable energy sources is getting higher, the risk of oscillations and resonance is growing, leading to instability of voltage levels. The voltage change needs to be continuously monitored and controlled. This scenario places the focus on the dynamics of voltage in a Low Voltage (LV) or Medium Voltage (MV) feeder. In the implementation of the Dynamic Voltage Stability Monitoring (DVSM) in a LV feeder, the two main components are Secondary Substation Automation Units (SSAU) and the inverters (electronic power converters).

SSAU hosts the voltage stability algorithm as a software component, and this program behaves as a coordinator gathering the information from the inverters to compute stability margins and send back control commands back to the inverters to modify the behaviour of the inverters. The SSAU performs the evaluation of stability margins once an hour for each inverter.

A Wideband System Identification (WSI) tool is used for the measurement of the impedances. There are two places where the WSI tool can be placed in the DVSM concept, either locally in the inverters, or centrally in the substations. In case that WSI tool is placed in the inverter, communication data volume between the substation and the inverter will be low. The message size per inverter will be 400 Bytes. On the other side if the WSI tool is placed in the substation, communication data volume will be high. The message size per inverter will be 320 kBytes.

The WSI tool is a computationally expensive algorithm since it requires high memory and complex mathematical routines such a Fast Fourier Transform (FFT) and complex curve fitting for system identification through the impedance coefficients are obtained. Therefore, the placement of WSI becomes critical. If the communication system can transmit large quantity of data, then it is optimal to place the WSI tool in the SSAU.

For further details about DVSM scenario please see Annex A.2.

Table 3-5 presents the minimum high-level ICT requirements to effectively run the DVSM.

Table 3-5: ICT communications requirements for DVSM

ICT Aspect	DVSM
Req-DVSM-endPoints	400-500 endpoints in urban areas
Req-DVSM-latency	Less than 200 ms
Req-DVSM-sampleRate	Every 2 – 5 minutes, DVSM monitoring to be performed
Req-DVSM-volume	400 Bytes if WSI tool is hosted in the inverter, 320 kBytes if WSI tool is hosted in SSAU
Req-DVSM-reliability	Incomplete or distorted messages must be checked and re-transmitted.
Req-DVSM-security	The Virtual Output Impedance (VOI) calculation takes place within the SSAU and the coefficients are transmitted to the inverter. This data needs to be

	secured.

1.17.2 Timescales and preconditions relevant to the commercial scale use of Dynamic Voltage Stability Monitoring (Sriram)

DVSM prototype software is prepared and deployed on the prototype electric circuit board in the lab. The prototype could be turned into the commercial product.

To allow the inverter to inject perturbations in energy networks, a new network code needs to be defined. The network code has to define how many perturbations are needed. The number of needed perturbations can vary from country to country. The adoption of the new network code depends on individual DSOs, but it is foreseen that the new network code could be defined within 5 years.

The communications in DVSM scenarios are needed. Generally, the communications requirements can be fulfilled by several existing network technologies. However, the voltage control quality is higher when the communication latency is lower.

1.17.3 ICT solutions

Choice of the protocols for the reliable communication

The Virtual Output Impedance (VOI) control coefficients are critical for the inverter to emulate its impedance behaviour in a stable way. Losing any VOI coefficient while transmission from SSAU to the inverter may cause critical instability problems. Thus, data loss is critical for DVSM scenario.

Protocols such as User Datagram Protocol (UDP) and Sampled Values (SV) are not suitable to use in DVSM scenario since successful delivery of messages is not guaranteed. UDP is connectionless, has no handshaking and thus does not provide any guarantees for message delivery or ordering. SV also does not provide message delivery reliability as it is based on Send and Forget methodology.

In opposite protocols that guarantee successful message delivery such as Message Queuing Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP) are recommended. These protocols were tested in the lab tests.

Communications protocol lab tests on the 5G Networks

Critical communication parameters in the DVSM scenarios are communication reliability and latency. In the lab test, packet latency was measured for different Quality of Service (QoS) levels in MQTT. In addition, different packet transmission rates were utilised.

The tests were conducted on the Enterprise 5G-ready mobile network installed in the laboratory at E.ON Research Institute in RWTH University in Aachen. In the test, applications deployed on the mobile user equipment and in the mobile core network were communicating between itself via tested mobile network infrastructure. Further details about the test systems infrastructure, test cases and test methodology can be found in D5.8, D4.6 and D5.9.

In order to test the effect of QoS parameter of MQTT protocol to the latency, the messages were sent at three different rates (1, 10 and 100 messages per second) for two different QoS values (0 and 1), and the latencies were measured. MQTT QoS level 0 guarantees a best-effort delivery whereas MQTT QoS level 1 ensures the message is delivered at least once.

Figure 3-1 shows the measured latencies on the Enterprise 5G-ready test system. When the latency results of QoS level 0 and 1 were compared per rate, no significant difference was observed for the rate of 1 and the rate of 10. This can be explained with the fact that the test was conducted in the well-controlled lab environment with no disturbances by other traffic and used traffic channels with high bandwidth. In addition, MQTT protocol was running via Transport Control Protocol (TCP) protocol that secures reliable data transmission.

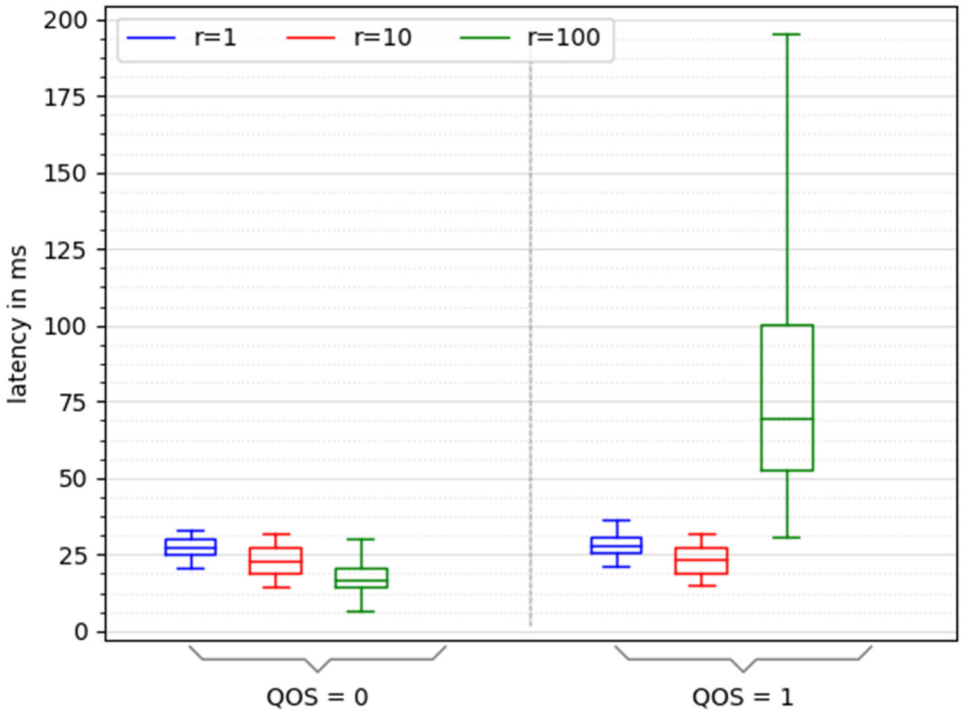

Figure 3-1 MQTT protocol latency for QoS 0 (fire-and-forget) and QoS 1 (at least once) measured on the Enterprise 5G-ready test system

For the rate of 100, however, the mean latency increased from 15 ms to 70 ms. The reason for the mean latency increase might be that the sender was sending the message multiple times if the QoS is set to 1 in order to assure the delivery of the message. Hence, for the transmission at a high rate of 100, the repetition of the message by the sender could increase the load on the underlying buffers and caused a higher latency.

Relationship between communications latency and grid impedance dynamics

Communications latency significantly influences how frequently dynamics of voltage will be monitored and controlled in LV or MV feeder. The lower the latency the control of voltage dynamics will be finer. However, the voltage dynamics control frequency is closely related to the grid impedance change dynamics. They have to be in balance in order to achieve the optimal functioning of the DVSM control. E.g., increase of the voltage dynamics control frequency, that is already much higher than the grid impedance change dynamics, will not improve the power grid quality.

The typical expected frequency of the voltage dynamics control, when 5G network is utilised, can be determined taking into consideration the following assumptions:

- The latency of the first Pseudo-Random Binary Sequence (PRBS) injection signal from SSAU to the inverter is 1ms.
- The time for the collection of data during noise injection in the inverter is 200ms, plus impedance coefficient extraction is 10ms.
- The latency of the grid impedance coefficient signal from the inverter to SSAU is 1ms.
- The Virtual Output Impedance (VOI) coefficient calculation takes 10ms.
- The latency of VOI coefficient signal from SSAU to inverter is 1ms.
- The average number of houses per SSAU is 500. We assume that all houses will be equipped with RES.

The following Table 3-6 shows typical expected voltage dynamics control frequencies when 3G, 4G and 5G mobile networks are utilised.

Mobile Network Technology	Average Latency [ms][2]	Voltage Dynamics Control Interval [min]
3G	200	6.8
4G	100	4.3
5G	5	2

Table 3-6: Typical expected voltage dynamics control frequencies for different mobile network technologies

According to Table 3-6, it is observed[3] that the latency will become critical factor depending on how fast the grid impedance can change. The grid impedance is dependent on network topology, cable parameters and dynamics of the inverters and loads. With improvement in semiconductor technology such as Silicon Carbide (SiC) and Gallium Nitride (GaN) devices, the switching frequency of power converters are expected to rise thus enabling faster dynamics. Therefore, the grid impedance change can be much faster in the future, and the communication technology with low latency will become critical.

Using Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms

In order to reduce latency over the wireless link, 5G Edge Cloud can be used in the architecture of appropriate communications solutions enabling usage of slower LTE network and hosting of the voltage calculation algorithm close to the assets.

Different DVSM solutions can be considered depending on allocation of DVSM resources in the edge cloud. In this section, three deployment scenarios are elaborated that are based on resources allocation on the edge device, the access edge cloud and the aggregation edge cloud:

- DVSM resources allocated on the edge device

  This scenario is highly futuristic because it assumes highly distributed architecture, self-maintaining network, and exclusion of the SSAU units.

- DVSM resources allocated on the access edge cloud

  The DVSM algorithm would be deployed on the access edge cloud collocated to the SSAU. Because distances between 5G radio base stations and distances between SSAUs are the same both in urban and rural areas, it can be assumed that the power grid cloud will be collocated to the mobile network edge cloud. Optionally, both mobile network and power grid applications can be deployed on the same edge cloud.

  The DVSM technique will be deployed on one SSAU unit and connected devices (inverters). The average number of devices connected to the SSAU unit will be 500 in urban, or 250 in rural areas assuming that all existing devices will be connected. This assumption is made based on the fact that if a higher number of devices are connected to the SSAU, the voltage management will be better. Prosumers can be motivated to provide the data to DSO for the voltage management purposes through the benefits from ancillary services.

  One DVSM solution deployed on one SSAU unit with its connected devices can work independently as a unit. Accordingly, DVSM would be deployed gradually in steps. The roll-out of DVSM through the entire power network is expected to take 20 to 30 years.

[2] Approximate average unidirectional latencies for 3G and 4G technologies as specified in https://www.cablefree.net/wirelesstechnology/4glte/lte-network-latency/

[3] With usage of 5G, we gain the best power quality monitoring of the grid. In the moment we cannot say if 4G and 3G communications can provide satisfiable control because it depends on how fast grid impedance can change what we don't know at the moment. Grid impedance change is possible to measure in power grid with the WSI tool.

- DVSM resources allocated on the aggregation edge cloud

  The DVSM algorithm would be deployed on the aggregation edge cloud. The aggregation edge cloud is typically two network hops from its intended users but is still much closer to them than the centralised cloud data center. This solution can be applied in both urban and rural areas.

  The aggregation edge cloud solution would be more cost-effective solution especially in urban areas as less edge cloud nodes would be used. On the other hand, stringent security requirements need to be fulfilled because the same cloud infrastructure would be shared by different DSOs.

  DVSM deployment in the power network would be gradual as in the case of deployment on the access edge cloud. However, the deployment would take shorter period comparing to the deployment on the access edge cloud.

- DVSM resources allocated on the aggregation edge cloud (C-RAN)

  One example of DVSM deployment on the aggregation edge cloud is described here, i.e., the deployment on the Cloud RAN (C-RAN). As C-RAN is two network hops from its intended users, the same conclusions as for the aggregation edge cloud deployment apply for C-RAN deployment.

  C-RAN radio access functions can run in the C-RAN cloud 20-40km away from radio base station. In this way C-RAN cloud can communicate to devices located kilometres away from the cloud. Note that very low latencies still apply in the communications between devices and the cloud resources (unidirectional delay of 2ms). In cause of simplicity it is assumed that C-RAN cloud covers a region of 50km in diameter. In this region up to 50 SSAUs can be located in urban area. Considering that each SSAU connects up to 500 RESs, one edge cloud would serve up to 25,000 RES units.

In addition, the following ICT solutions for DVSM scenarios that are common for several other scenarios are listed here and described in detail in Chapter 4:

- Providing communications links to new end-points in the energy system
- Ensuring end-to-end latency of 10 to 20ms
- Use of communications friendly protocols to maximise the reliability of the communications
- Network Slicing for energy provider control of QoS and security features
- Use of public 5G networks without network slicing and public 4G LTE networks
- Using Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms
- Use of private 4G or 5G networks
- Mobile networks for massive IoT communications

1.18 Summary of ICT Requirements for Voltage Control

The following Table 3-7 shows two voltage control scenarios elaborated in this deliverable and the ICT requirements most relevant for the scenarios (latency, reliability, etc.).

Energy Scenarios / ICT Requirements	Active Voltage Management	Dynamic Voltage Stability Management
Architecture	Centralised/Hybrid	De-centralised
End-Points	<10,000(centralised)/1000(hybrid)	<1000

Latency	<1095ms	<10ms
Sampling Rate	Typically 1 per second	NA
Data Volume	75-80Bytes	0.4-320kBytes
Reliability	99.99%	99.99%
Security	High	High

Table 3-7: Summary of ICT requirements for Voltage Control Scenarios

In the AVM scenario, two of the three energy solution architecture options are considered. Decentralised architecture is not considered because it does not require communications. On the other hand, one energy solution architecture is provided in DVSM scenario.

The End-Points parameter shows that the concentration of the devices in both scenarios is rather equal. Note that for the hybrid and decentralised architectures, a smaller number of devices located in geographically smaller areas communicates to the concentration point at which the solution logic is deployed. In the centralised solution architecture, a high number of devices dispersed over a large area is communicating to the common control point.

The Latency parameter indicates the transmission time for a measurement or control signal to be sent from point A to point B over the communications network. In the AVM scenario, this time includes the end-to-end transport of data over radio interface, processing in base station, transport over the backhaul network, and processing in core network. In DVSM scenario, this time includes the end-to-end transport of data over radio interface, and processing in the edge cloud collocated to the base station. It is observed that latency is critical factor in DVSM scenarios.

The sampling rate is not applicable in DVSM scenarios because the control centre communicates to the measurement devices sequentially. In each communication cycle, several signals are exchanged between the control center and the device. The cycle is repeated every 2 minutes when 5G communications are utilised.

The Data Volume is the maximum size of a standard message transmitted between end-points, including overhead for addressing, time stamps, authentication and authorisation, encryption, et al. Typically, the size of messages in energy networks is very small. This is the case for both voltage control scenarios. It should be noted the difference in the message size in DVSM scenarios. Message size depends on the placement of DVSM algorithm either on the device or in the control center.

High reliability of the communications is requested in each scenario represented with ‘four nines’ meaning that maximal allowed communications system downtime per month is 4 minutes and 23 seconds, or 52 minutes and 36 seconds per year.

In both scenarios, high communication security is needed.

4. Relationship between 5G ICT Solutions and Voltage Control Scenarios

This section describes 5G ICT solutions for the voltage control scenarios. The relationship between 5G ICT solutions and the voltage control scenarios is indicated in Table 4-1. Note that 5G ICT solutions are not provided in AVM Scenario 2 because the communications are not needed in that scenario.

Table 4-1: Relationship between 5G ICT Solutions and voltage control scenarios

Energy Scenarios / 5G ICT Solutions	AVM		DVSM
	S1	S3	
Providing communications links to new end points in the energy system	X	X	X
Ensuring End-To-End latency of 10 to 20ms			X
Use of communications friendly protocols to maximise the reliability of the communications	X	X	X
Network Slicing for energy provider control of QoS and security features	X	X	X
Use of public 5G networks without network slicing and public 4G LTE networks	X	X	X
Using Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms		X	X
Use of private 4G or 5G networks		X	X
Mobile networks for massive IoT communications	X	X	X

In further text, 5G ICT solutions listed in Table 4-1 are described in detail.

Providing communications links to new end points in the energy system

Wireless communications systems, such as 5G, will offer cost-effective and easy to deploy solutions to supply communications over shorter distances to connect individual new assets which are part of the voltage control scenario to fixed networks. In a mobile wireless network, it is normal to have a fibre optic cable connecting each base station and antenna to the backbone of the 5G and general communications transmission system. This means that only the distance between the sending device at the new asset (RES) and the nearest 5G base station antenna is actually communications over the air. Once the signal reaches the base station, it is transmitted further within the 5G and other communications networks to the intended receiver (central controller) over fixed communications links.

Ensuring End-To-End latency of 10 to 20ms

To achieve end-to-end latencies under or equal to 10ms 5G wireless links or fixed cabled connections are very likely to be required as a solution.

Latencies of under 20ms can be achieved by 4th Generation LTE wireless networks. The configuration of the network in the exact locations would have to be investigated to check that the network in question could provide these latencies for each individual link.

Use of communications friendly protocols to maximise the reliability of the communications

The packets to be transmitted are probably of small size, of the order of magnitude of several hundred kilobits of information. The protocols used by the energy systems should preferably be chosen so that they optimise the efficiency of the use of the wireless communications channel. Examples of commonly used energy protocols which make efficient use of wireless communications channels include MQTT and AMQP and other TCP based protocols. Investigations by Ericsson of energy protocols concluded that the use of the Sampled Value protocol is not appropriate as this protocol does not confirm the arrival of packets. Other energy protocols, such as 61850 GOOSE can generate communications problems as it produces bursts of traffic which can suddenly overload wireless channels and cause delays in transmission.

Network Slicing for energy provider control of QoS and security features

Additionally, if the energy provider wants to ensure the quality of service of the communication and the security of the communications on an end to end basis, they could use Network Slicing features of 5G networks to set their own priorities for communications resources reserved for their slice and to use whatever communications security mechanisms they consider appropriate. The 5G networks used could be privately owned by energy providers or could be public 5G networks, or any combination of the two.

Using Distributed Edge Cloud features to reduce the latency requirements and provide local hosting of algorithms

In order to reduce the requirements on latency over the wireless link, so that an LTE or slower wireless link could be used, and also potentially, to enable hosting of the frequency calculation algorithm close to the assets, 5G Edge Cloud could be included in the architecture of appropriate communications solutions.

Use of public 5G networks without network slicing and public 4G LTE networks

In a public 4/5G network, the bandwidth available is shared between many users without reservation of network resources resulting in the situation that if there is very heavy traffic load on the network, it is possible that network congestion may result in reduced reliability and increased latency of the communications. Complete loss of individual packets is possible in such rare circumstances.

Use of non-public 4G or 5G networks

A non-public (sometimes also called private) cellular network could be deployed by a DSO or Transmission System Operator (TSO) to provide part or all of the communications links required to use the scenarios defined above. Non-public networks offer the advantage that the owner has complete control of the priorities, security, configuration and access to the network. Public networks can be used to completement the use of no-public wireless networks, for example, enabling single remote locations to be reached by public networks.

Solutions such as the recently introduced **Ericsson Industry Connect** solution[4], based on 5G, provide cost-effective indoor and limited outdoor communications for use in industrial environments and could contribute to communications solutions for this use case if the devices to be connected are located indoors. The solution acts as an indoor repeater enabling 4G and 5G communications to be used indoors in situations where the 4 or 5G signal is too weak to be used without a repeater. This enables a single type of communications network with a single definition of its security and other characteristics to be used for a complete solution giving economy of scale to the operation and maintenance of the communications.

Mobile networks for massive IoT communications

When communication latency is not critical requirement, besides 5G other network technologies for massive IoT type communications can be utilised like: EC-GSM-IoT, LTE-M and NB-IoT. 4G and 3G mobile networks can also be considered if the requirements can be fulfilled in such cases.

If components requiring communications are in very deep basements (more than 2-3 levels below ground, or in rooms with particularly heavy concrete walls, the penetration of the LTE or NB-IoT

[4] See https://wcm.ericsson.net/en/internet-of-things/industry4-0

communications devices may require the deployment of small repeaters, with cabled connections, to ensure reliable communications.

5G networks will also provide excellent communications solutions for such scenarios. Repeaters for the indoor use of 5G spectrum will be introduced to the market in coming years ensuring that 5G will operate in deep basements and in buildings hosting critical infrastructures with reinforced walls.

5. Conclusion

A stable voltage level is essential to prevent smart grids from disturbances or even outages. This deliverable shows that some scenarios have demanding requirements for high-performance, reliable, secure, and fast communications networks, to ensure that the voltage control algorithms can swiftly respond to any deviations in the grid. The number of energy generation units will grow drastically, and with it the number of end-points and control units in the network. Applicability of ICT communication aspects were thoroughly considered through all voltage control scenarios. The following key ICT communications aspects, among many, were identified and considered: number of end-points, communication latency, reliability and security.

Wireless communications systems, such as 4G and 5G, will offer cost-effective and easy to deploy solutions to supply communications over shorter distances to connect individual new assets which are part of the voltage management scenario to fixed networks. The number of devices in the voltage control scenarios that need to be connected is high.

Latency of the communication in the voltage control scenarios varies over a wide range. Nevertheless, the latency smaller than 10ms will improve quality of the voltage control. To achieve end-to-end latencies under or equal to 10ms, 5G wireless links or fixed cabled connections are very likely to be required as a solution. Latencies of under 20ms can be achieved by 4th Generation LTE wireless networks.

In majority of analysed cases excluding those requesting very low latency of 10 to 20ms, wireless networks for critical IoT type communications as EC-GSM-IoT, LTE-M and NB-IoT can be used. These networks have improved outdoor coverage and significantly improved indoor signal penetration to reach deep indoors. Other LPWA network technologies (LoRA, Sigfox) were not considered in this study. Usage of other LPWA network technologies could be the topic for future research. The research should focus on the following aspects: performance, reliability, security, coverage and economics.

Reliability is critical component of the voltage control. 5G brings new features like network slicing and distributed cloud computing ensuring reliable functioning of the voltage control. Non-public networks that are getting more and more on popularity provide to owner full control over the communication infrastructure including reliability. Furthermore, TCP based protocols like MQTT and AMQP provides reliable data transmission by design.

6. References

[1] Ericsson White Paper, “Cellular IoT Evolution for Industry Digitalization”, GFMC-19:000017 UEN, January 2019.

[2] GSMA, "Mobile IoT in the 5G Future," April 2018.

[3] Ericsson White Paper, “5G deployment considerations”, EAB-18:001198 Uen Rev.B, 2018.

[4] Ericsson White Paper, “5G security – enabling a trustworthy 5G system”, GFMC-18:000078, March 2018.

[5] J. Davis, P. Shih and A. Marcham, "State of the Edge 2018: A Market and Ecosystem Report for Edge Computing," Structure Research, 2018.

[6] A. Checko, M. S. Berger, G. Kardaras, L. Dittmann and H. Christiansen, "Cloud Radio Access Network architecture. Towards 5G mobile networks," Technical University of Denmark (DTU), 2016.

[7] Ericsson White Paper: “5G Systems, Enabling the transformation of industry and society”, UEN 284 23-3251 rev B, January 2017

[8] Ericsson Technology Review: “Distributed cloud”, November 2018

[9] ETSI/SAGE: “Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification”, Version: 1.6, June 2011. Available at https://www.gsma.com/security/wp-content/uploads/2019/05/eea3eia3zucv16.pdf

[10] ETSI/SAGE Specification: “Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification”, Version: 2.1, March 2009, Available at https://www.gsma.com/aboutus/wp-content/uploads/2014/12/uea2uia2d1v21.pdf

[11] IETF RFC5930 “Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol”, Hangzhou H3C Tech. Co., Ltd., NSS. Murthy, July 2010. Available at https://tools.ietf.org/html/rfc5930

[12] IETF RFC4493, “The AES-CMAC Algorithm”, University of Washington, Samsung Electronics, Nagoya University, June 2006. Available at https://tools.ietf.org/html/rfc4493

[13] IETF RFC2104: “HMAC: Keyed-Hashing for Message Authentication, IBM, UCSD, February 1997”. Available at https://www.rfc-editor.org/rfc/rfc2104.txt

[14] Elliptic Curve Cryptography Version 2.0 (2009), SECG SEC 1 specification, available at: http://www.secg.org/sec1-v2.pdf

[15] NESAS – Network Equipment Security Assurance Scheme (2018), GSMA, available at: https://www.gsma.com/aboutus/leadership/committees-and-groups/workinggroups/fraud-security-group/network-equipment-security-assurance-scheme

[16] 5G-ACIA: “5G Non-Public Networks for Industrial Scenarios”, July 2019

[17] 3GPP: “TS 23.251 v15.1.0 Network sharing; Architecture and functional description”, 2018

[18] R. D. Middlebrook, “Input filter considerations in design and application of switching regulators,” pp. 366–382, 1976.

7. List of Figures

8. List of tables

9. List of Abbreviations

3GPP	3rd Generation Partnership Project
5G	Fifth generation cellular network technology
5GC	5G Core
AES-CMAC	Advanced Encryption Standard Cipher-based Message Authentication Code
AES-CTR	Advanced Encryption Standard Counter
AMQP	Advanced Message Queuing Protocol
AVM	Active Voltage Management
BBU	BaseBand Unit
C-RAN	Cloud Radio Access Network
CAT-M	Category M
DER	Distributed Energy Resources
DERMS	Distributed Energy Resource Management System
DSO	Distribution System Operator
DVSM	Dynamic Voltage Stability Monitoring
EAC	Exploitation Activities Coordinator
EC-GSM-IoT	Extended Coverage-Global System for Mobile Communications-Internet of Things
ECIES	Elliptic Curve Integrated Encryption Scheme
EIR	Equipment Identity Register
E-UTRAN	Evolved Universal mobile telecommunication system Terrestrial Radio Access Network
FFT	Fast Fourier Transform
FWA	Fixed Wireless Access
GSMA	Global System for Mobile communications Association
HMAC-SHA-256	Hash-based Message Authentication Code Secure Hashing Algorithm 256-Bits
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
LPWA	Low Power Wide Area
LTE	Long-Term Evolution
LTE-M	Long-Term Evolution for Machines
LV	Low Voltage
M2M	Machine to Machine
MBB	Mobile BroadBand
MQTT	Message Queuing Telemetry Transport
MTC	Machine Type Communications
MV	Medium Voltage
NB-IoT	NarrowBand Internet of Things
NESAS	Network Equipment Security Assurance Scheme
NR	New Radio
NSA	Non-Stand-Alone
PRBS	Pseudo-Random Binary Sequence
PV	Photovoltaic (power generation unit)
QoS	Quality of Service

RAN	Radio Access Network
RES	Renewable Energy Sources
RRH	Remote Radio Head
SA	Stand-Alone
SBA	Service Based Architecture
SCAS	SeCurity Assurance Specification
SIM	Subscriber Identity Module
SNOW 3G	Word-based synchronous stream cipher with name SNOW
SSAU	Secondary Substation Automation Unit
SV	Sampled Values
TCP	Transport Control Protocol
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TSO	Transmission and System Operator
UDP	User Datagram Protocol
URLLC	Ultra-Reliable Low Latency Communication
V2G	Vehicle-to-Grid
VOI	Virtual Output Impedance
VVC	Volt-Var Curve
WiFi	Wireless Fidelity (local area wireless technology)
WP	Work Package
WSI	Wideband System Identification
ZUC	Cryptographic algorithm with name ZUC

Annex

A.1 Volt-Var Curve Execution

The execution of the AVM algorithm, and more accurately, the Volt-Var Curve (VVC), which is the actionable output from the algorithm, involves an investigation of a set of suitable architectures or approaches. From an ICT perspective, this will allow an effective execution in both a simulation environment, and in trial site implementations.

With reference to deliverable D1.3 section 2.3 the author refers to centralised, decentralised and distributed approaches from an electrical engineering perspective. In order to fully explore the potential execution of the AVM, it is important to discuss these architectures in terms of information technology, from a distributed systems approach. This approach has its foundation in communications and networking and comprises of the interconnection of heterogeneous physical and virtual components distributed across a LAN or WAN for the purpose of data transfer and system control.

The following sub-sections will detail three architectures identified, a **Centralised** model, a **Decentralised** model and a **Hybrid-Edge Computing** model, from the perspective of their mechanics, topological structure and high-level ICT requirements. The main differences between each architecture are in terms of the geographical distance between the execution of the VVC and the inverter, and the autonomy of each RES unit from a central control point in terms of voltage management and the granularity of control.

A.1.1 Centralised Volt-Var Curve Execution

The diagram in Figure A-1 illustrates the topology and data flow of a centralised model of the execution of the AVM technique. In this case the Volt-VAR curves for the trial sites would be stored on the cloud server at a central geographical control centre with reference to their specific device or location. The execution will take place on a voltage value contained in the payloads sent from the target site via an MQTT broker running on a mobile network connection with the output of this being the sending of a Reactive Power (Q) set point to the target RES site. This approach has a focus on the communications-based focus as the readings are sent to the cloud implementation for processing. This approach requires full time communication and reliance on a central control centre with potential large geographical distance between the target inverter and the execution of the VVC. These geographical distances and the potential to have a large number of devices under one central control point may have impact on the following ICT criteria.

Implementing the AVM with a centralised approach will have a high level of latency. This is due to the messages having to travel long distances between Central Controller and RES Unit. The high frequency of communications from multiple sites can play a factor into the response time too. This will also mean that a high level of information reliability is needed, as many RES devices are dependent on this central server. More computing resources will be required to implement techniques to handle the large number of messages and to ensure none are lost. The data volume would be of medium level, because while the message itself is small, there is overhead involved, such as authentication and encryption. Communication will occur over public networks, which means messages will require high levels of security, because if this centralised system is compromised it can have a severe impact. The data sent and received has to be confidential and trustworthy. MQTT allows for messages to be encrypted with no significant loss in performance. The MQTT broker will also require authentication in order to send/receive messages.

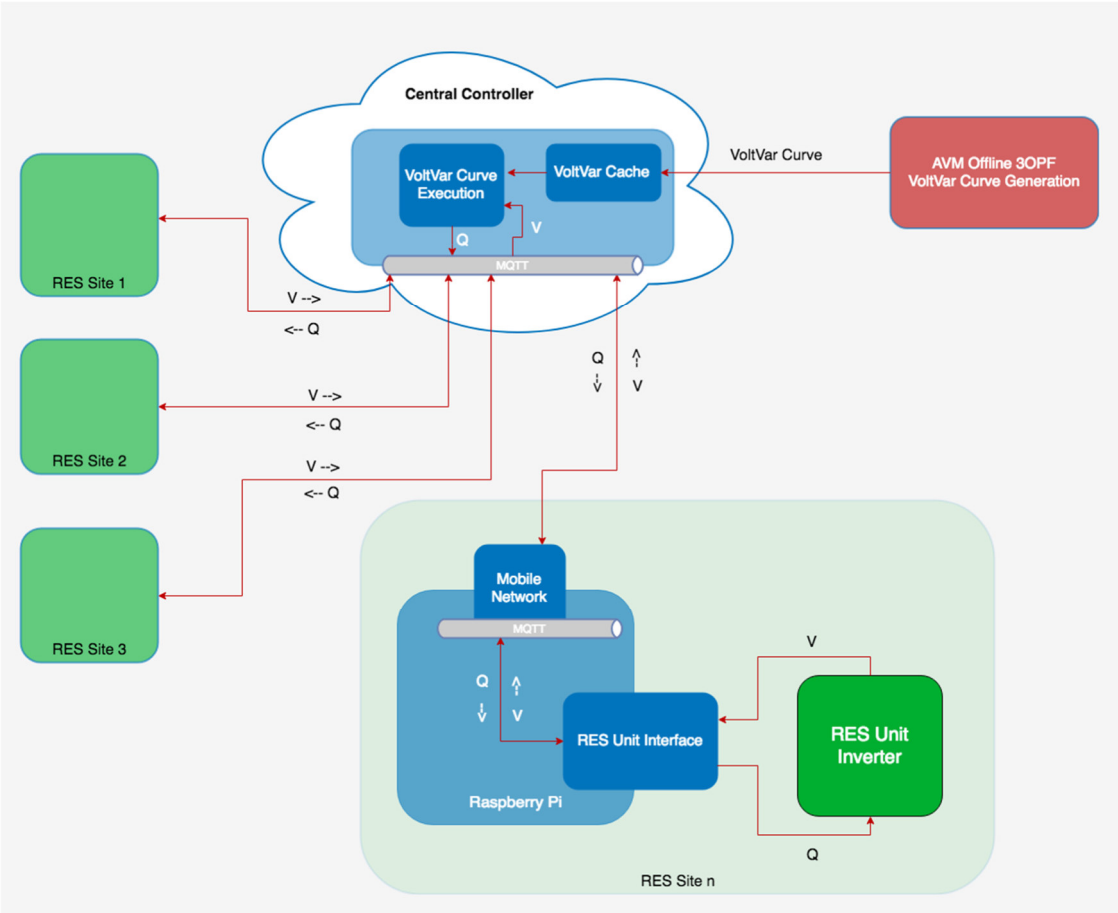

Figure A-1 Centralised AVM Execution Architecture

A.1.2 Decentralised Volt-Var Curve Execution

The diagram in Figure A-2 illustrates the topology and data flow of a decentralised model of the execution of the AVM technique. While being managed by the central controller, its only communication is to receive the VVC for execution either on the Raspberry Pi device or for direct input into a smart inverter that would have the native capability and interface to process the VVC. This approach adds a layer of autonomy from central control due to the fact that while the RES site has the VVC it is capable of running independently. The only other communication required would be for an update to the VVC algorithm for a specific RES Unit. From a central cloud perspective, while the VVC execution is being carried on the edge, the physical distance between the inverter and the VVC execution has a lesser impact from a latency perspective, but the potential number of managed objects (RES Units) would remain the same highlighting a potential scalability issue in this approach. Given that, there is an extra layer of computing on the hardware at the RES Site, which is the potential updating of a VVC at each RES Unit. The mapping and sending of a VVC to the correct RES unit is executed at the cloud controller level. The impact of the above requirements, from an ICT perspective, can be evaluated under the following criteria.

A decentralised approach involves having a Raspberry Pi to enable communication between the cloud service and inverter, perform calculations if needed or to simply upload the VVC to the inverter. Implementing this approach will ensure the smallest level of latency due to the VVC being as close as possible to the RES Unit. Frequency of communication is rather low, as each Raspberry Pi is in contact with only one RES Unit at any time, so the demand on computing resources is minimal. However, a decentralised approach will require a Raspberry Pi to be manually installed at every RES Unit that does not have an inverter with mechanisms to receive and process the VVC natively. Information reliability can be kept low as only one RES unit will be affected if the Raspberry Pi is down. The data volume for communication between Raspberry Pi and inverter will be low, the message content will remain the same and the overhead will be minimal as this communication will occur over a direct ethernet connection. The data volume

between Raspberry Pi and cloud server will be at a medium level as these messages are sent over public networks where more overhead is required. This public communication is needed to update the VVC, but the frequency of this will be very low. As this will happen over a public network, secure MQTT communication will be needed. A medium level of security would be required, because one RES device can seriously affect the power supply in the local area. The communication to cloud server needs to be secured, but the edge device itself will need to be protected also. This is to prevent any tampering with the edge device hardware and to protect it from various weather conditions.

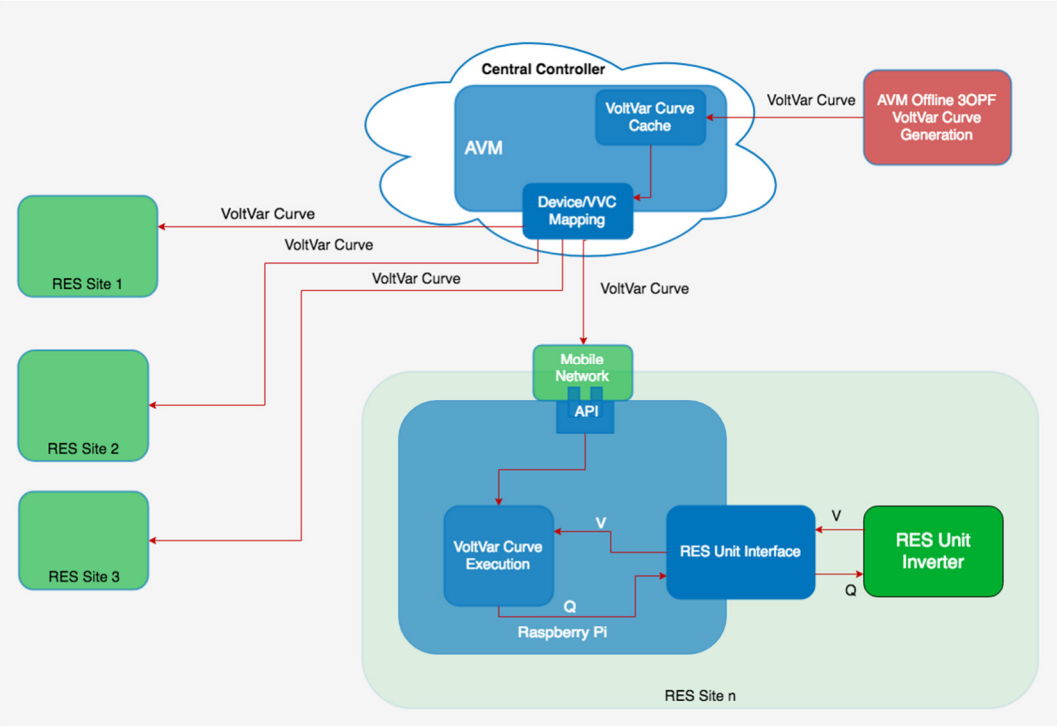

Figure A-2 Decentralised AVM Execution Architecture

A.1.3 Hybrid Edge Computing Volt-Var Curve Execution

Figure A-3 illustrates a high-level topological view of a hybrid implementation of the AVM technique using both a centralised and a decentralised approach:

- Centralised approach in terms of the initial creation of the VVC's
- De-centralised approach, or edge-computing application, deployed to regional cell tower entities with computational capabilities to control the orchestration and execution of the VVC's at RES sites in specific regions.

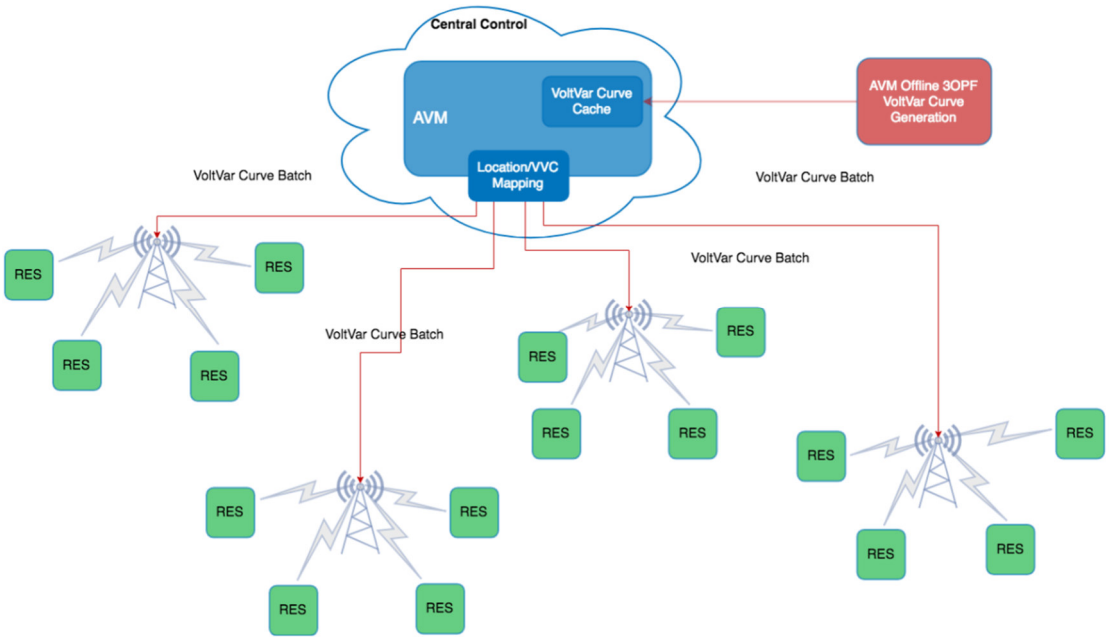

Figure A-3 AVM Hybrid Approach Architecture

The diagram in Figure A-4 details the data flow and components required for a hybrid approach at a regional level. The core component is a computing node at the edge of the communications network, co-located with the 5G radio base stations in the access network towers. The computing node has preconfigured knowledge of each distributed energy site in its area, including computational capabilities, connection details and the specific VVC. This site specific configuration can drive the level of computing required for each RES site and carry out the required computation accordingly. From the detail gathered in D5.2 it is clear that there are three levels of computational capabilities. These levels are, the inverter being capable of accepting a VVC, the setpoint calculation can be computed at the RES Unit using the voltage and VVC and the RES unit is only capable of sending voltage and receiving a setpoint value. To summarise this approach in terms of ICT requirements, we need to evaluate it on the following criteria.

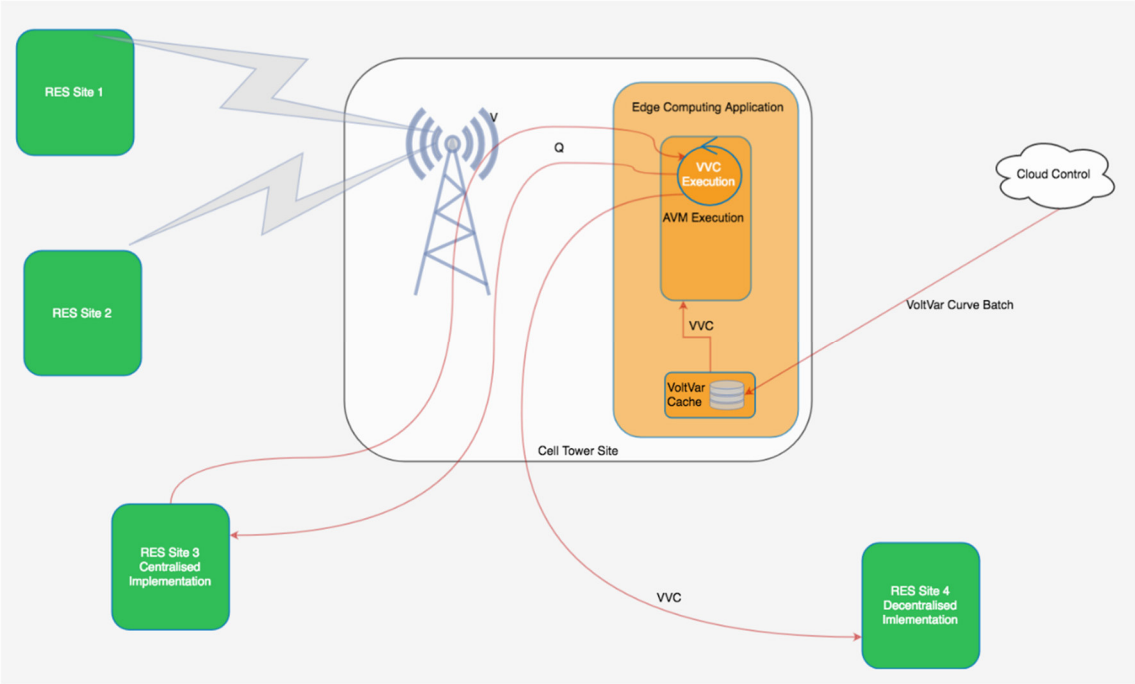

Figure A-4 AVM Hybrid Approach Regional Implementation

A hybrid approach can be seen to have a medium frequency of communication level, because it will have to manage multiple RES devices from multiple sites, but not on the same scale as a centralised system. The frequency of communication between edge node and cloud server would be rather low, as the server will need to send down multiple VVCs to the device. The latency would be low as there should not be a significant distance between cell tower site and RES site. Medium levels of information reliability are to be expected due to multiple RES Sites being dependant on the edge device. The data volume would be of medium level too, because while the message itself is small, there is overhead involved, such as authentication and encryption. The security level would be medium, it would have a serious impact on the RES devices in the immediate area. All communication is sent over a public network and must be secured. The edge device is more exposed than a centralised server, measures will be needed to prevent damage to the hardware.

A.2 Scenarios for Dynamic Voltage Stability Monitoring

A.2.1 Introduction to DVSM

This scenario places the focus on the dynamics of voltage in a LV or MV feeder, which is the rate of change in voltage. This change rate needs to be continuously monitored and controlled, that is the first derivative of the voltage curve in mathematical terms. If the first derivative is 0, then the voltage curve does not face any rate of change. In comparison to Sv_B, Sv_A is more preventive and proactive.

The Challenge: when the share of renewable energy sources is getting higher, the risk of oscillations and resonance is growing, leading to instability of voltage levels. Figure A-5 shows a scenario where this risk is visualised.

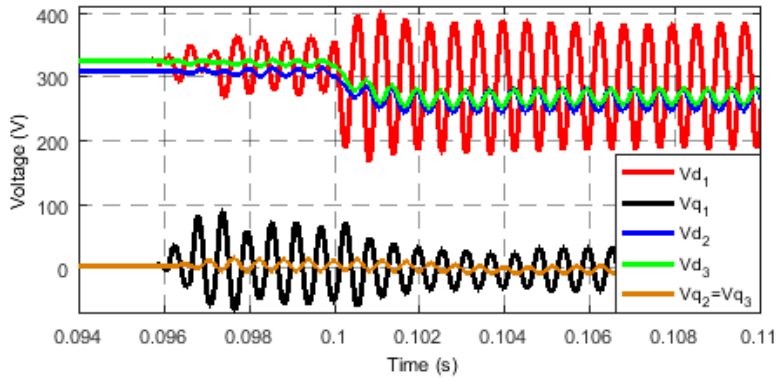

Figure A-5 Voltage oscillations and resonance in an LV feeder

As Dynamic Voltage Stability Monitoring (DVSM) is also concerned with the absolute voltage values in the grid, his approach is more complex and comprehensive than the Active Voltage Management described above. Figure A-6 shows the implementation of the Dynamic Voltage Stability Monitoring in a LV feeder setting. The key elements are the secondary substation automation units (SSAU) and the inverters (electronic power converters) connecting the distributed energy sources.

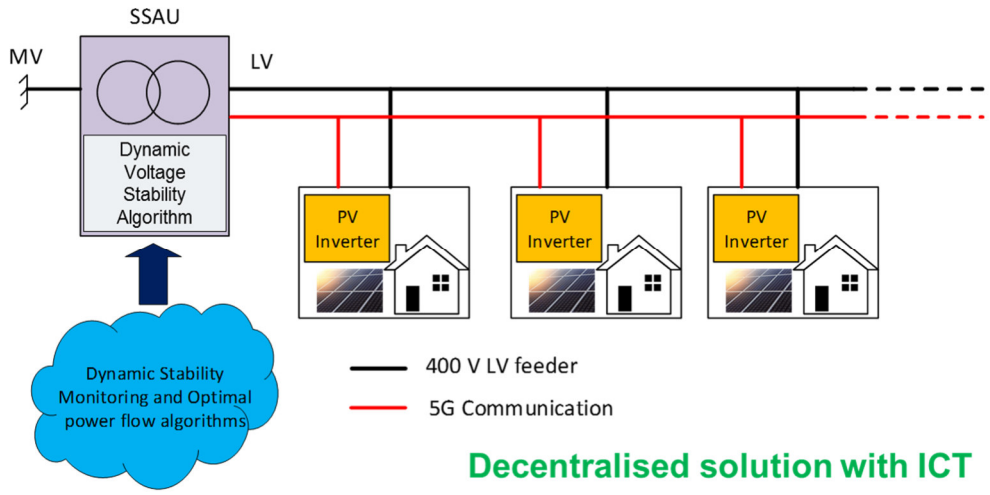

Figure A-6 Typical deployment of decentralised Dynamic Voltage Stability Monitoring

The secondary substation automation unit (SSAU) hosts the voltage stability algorithm as a software component, and this program behaves as a coordinator gathering the information from the inverters to compute stability margins and send back control commands back to the inverters. The SSAU performs the evaluation of stability margins once an hour for each inverter.

The approach in Figure A-7 is based on the Middlebrook theory [18] where the stability can be determined using the **inverter output impedance** and the **grid impedance** as input. See Figure A-7 below.

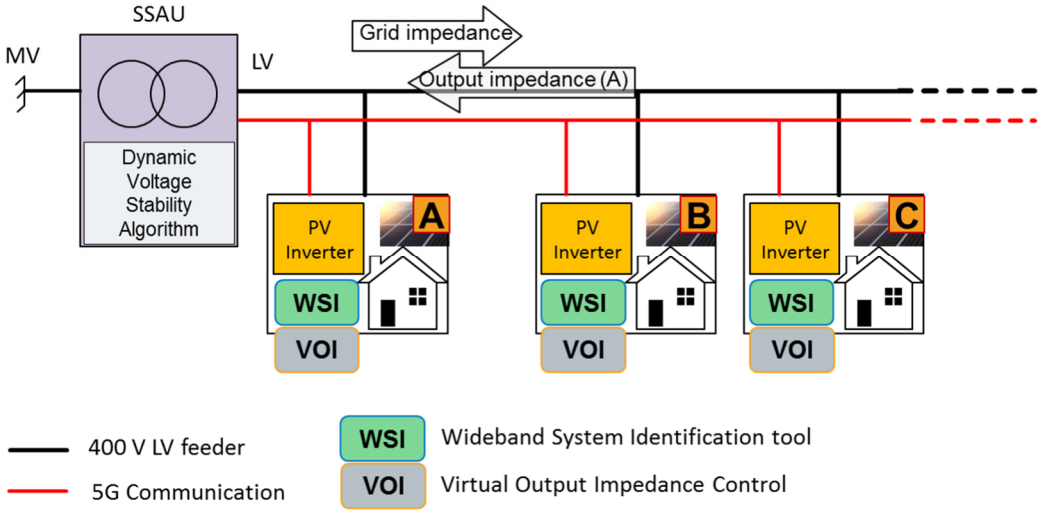

Figure A-7 Impedance monitoring and control

For the measurement of the impedances, a wide-band system identification (WSI) tool is present in the inverter. The WSI tool injects a pseudo-random binary sequence (PRBS) signal into the controller in the inverters and processes the incoming voltage and current measurements to determine the impedance.

In the DVSM technology, the SSAU intends to modify the behaviour of the inverter. For this purpose, the SSAU sends an initiation signal to Inverter A to use its WSI tool to measure the *grid impedance*. The inverter's *output impedance*, on the other hand, is mathematically modelled in the controller of the inverter. The output impedance of the inverter is a function of the physical parameters of the inverter such as power filter parameters and the control parameters. Therefore, at any given point during the operations, the controller of the inverter knows the output impedance of the inverter.

The coefficients of the identified grid and output impedance are sent back to the SSAU. The SSAU performs stability analysis based on the Middlebrook theory, computes the stability margins and, if required, sends back control commands to the virtual output impedance controller (VOI) of the inverter A. This process is repeated for Inverter B and furthermore for all other inverters present under the direct control of the SSAU.

A.2.2 Location of the WSI tool

There are two places where the WSI tool can be placed in the DVSM concept, either locally in the inverters, or centrally in the substations. See also D3.5.

A.2.2.1 WSI Tool Location in RES Inverters

- The controller of the inverter has the complete WSI algorithm. This includes the subroutines like PRBS noise generation, extracting the non-parametric impedance and parametric impedance identification.
- The Inverter uses communication to communicate only the identified impedance coefficients. Communication data volume is low.

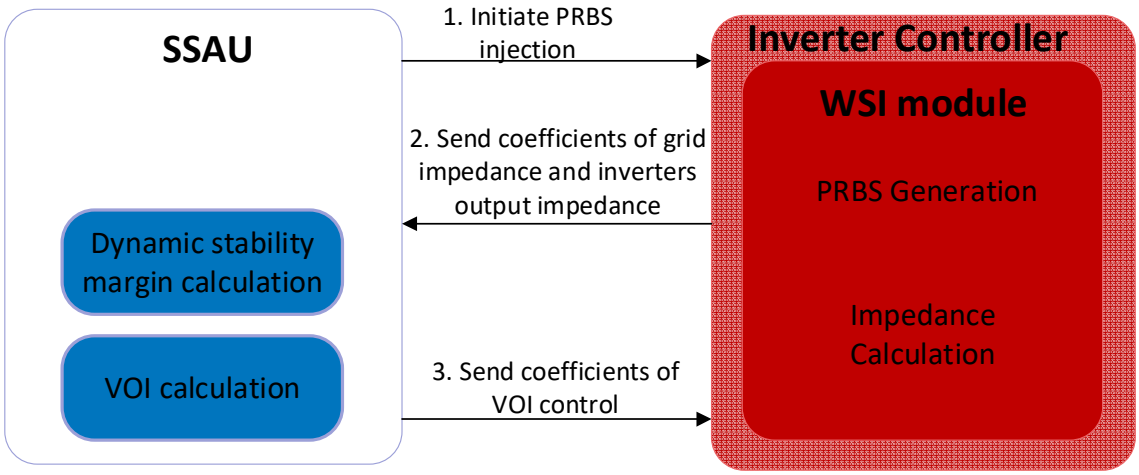

Figure A-8 System-level Integration of WSI located in Inverter

Considering that the process repeats for an inverter every 5 minutes.

Data Volume/Bandwidth

- Floating point (double precision) – 8 bytes per number
- Number of floating point numbers per inverter (considering VOI coefficients) – 100
- Number of inverters (1 Inverter per end-point) – 500
- Kilobytes per second – 8*100*500/(1024*300) = 1.3021 kBytes/s
- Kilobits per second – 10.41 kbits/s

A.2.2.2 WSI tool Located in SSAU

- The controller of the inverter has only the PRBS noise generation subroutine.
- The rest of the WSI functionalities such as extracting the non-parametric impedance and parametric impedance identification is performed in SSAU.
- The Inverter uses communication to send voltage and current data measured during the perturbation. Communication data volume is high.

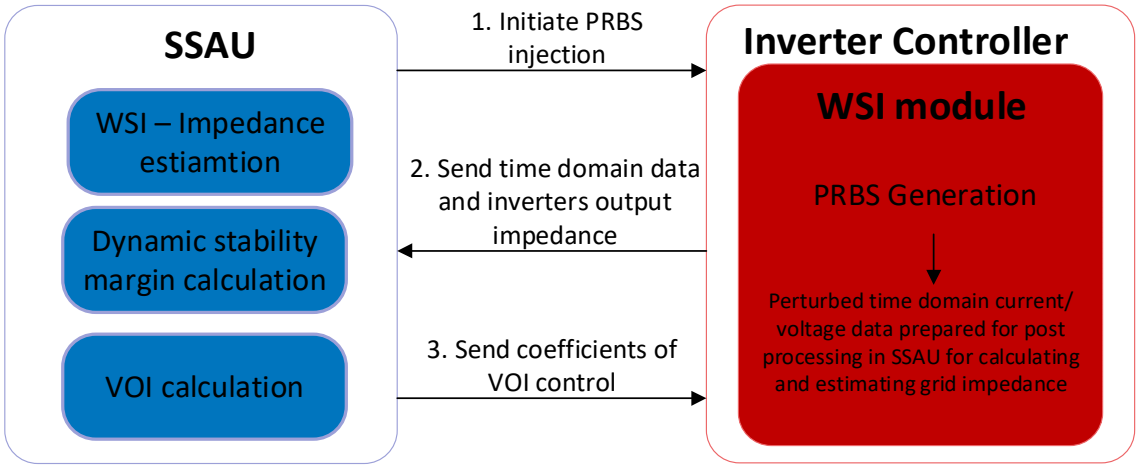

Figure A-9 System-level Integration of WSI when implemented in SSAU

Data Volume/Bandwidth

Considering the sampling frequency within the inverter controller of 50 kHz and the number of fundamental cycles (N) of the power system frequency of 50 Hz for which the measurements are recorded, the number of data points can be calculated as: Ns=N*50kHz/50 Hz.

- Floating point (double precision for coefficients) – 8 Bytes per number
- Number of floating point numbers per inverter (considering VOI coefficients) – 50
- Total bytes for all coefficients = 8Bytes*50 =400 Bytes
- Time domain data of perturbed signals – 2 Bytes per number
- Number of channels (Vd,Vq,Id,Iq) – 4
- Number of fundamental cycles N -10
- Number of perturbed time domain data - 10*50,000/50 =10,000
- Total bytes of perturbed time domain data – 10,000*4 channels* 2 bytes = 80,000 Bytes
- Overall total data - 80,000 Bytes (from time domain data) + 400 Bytes (Coeffcients) = 80,400 Bytes
- Number of inverters (1 Inverter per end-point) – 500
- Kilobytes per second – 80,400*500/(1024*300) = 130.86 kBytes/s
- Kilobits per second – 1047 kbits/s

A.2.2.3 Impedance Data

Dynamic Voltage Stability Management uses the *impedance* to control voltage levels. This applies to both measurements in the grid as well as to control commands if corrective actions are needed.

It is recommended to perform the impedance monitoring and control only for one inverter at a time, as inserting PRBS noise at many points of the grid may lead to noise overlay or interference.

The *grid impedance* matrix Z_{grid} consists of 4 components: $Z_{grid,DD}$, $Z_{grid,DQ}$, $Z_{grid,QD}$ and $Z_{grid,QQ}$. Each of these four elements consists of 12 coefficients with floating point numbers. For example, $Z_{grid,DD}$ consists of 12 floating point numbers. Therefore, the entire grid impedance matrix is represented by 48 floating point numbers. In this study, the authors round it off to 50 coefficients.

The inverter *output impedance* matrix Z_{out} consists of 4 components: $Z_{out,DD}$, $Z_{out,DQ}$, $Z_{out,QD}$ and $Z_{out,QQ}$. Similarly, there are 50 coefficients for the output impedance.

In the downlink direction, from the substation, the VOI control command coefficients that come from the SSAU contain 50 coefficients too. Note that the VOI control command has the same data format, it is essentially an impedance matrix too.

Therefore, in any cycle, the messages will exchange 50+50+50 (150) floating point numbers. The inverters are processed sequentially, and not concurrently. Therefore, it can take between two and four seconds for the process to complete for *one inverter*, and a typical LV feeder may have up to 100 inverters, it can take up to 200-400 seconds until the same inverter is monitored again.

For each cycle, 4 messages of approx. 150 floating point numbers are exchanged between SSAU and one inverter.