IDATE CONSULTING

Etude bibliographique : wireless communications

Etude réalisée pour Normandie AeroEspace

70051 – Novembre 2017 – version diffusable

Chef de projet

Frédéric Pujol

f.pujol@idate.org

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Normandie
AeroEspace
La passion de l'Excellence

Étude Bibliographique

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Étude Bibliographique

Table of contents

1 Structure and content of the report 10
1.1 Technologies covered in the report 10
1.2 Presentation of wireless technologies 11
1.2.1 Performances & TRL evaluation scale used in this report 11
2 Synthesis 13
3 Commercial mobile network technologies 17
3.1 Synthesis 17
3.2 Introduction 17
3.3 Performance of commercial cellular technologies 19
3.3.1 1st generation (1G) 19
3.3.2 2nd generation (2G) 19
3.3.3 3rd generation (3G) 21
3.3.4 4th generation (4G) 22
3.3.5 The case for cellular IoT 24
3.4 Geographical market 26
3.5 Norms and regulatory context 27
3.6 Level of security and threats 28
3.7 Main equipment manufacturers 28
3.8 Maturity level 29
3.9 Stakes regarding market and competition 29
3.10 Which evolution in the next five years 30
3.11 Maturity of the ecosystem in the years to come 32
4 Professional Mobile Radio technologies (PMR): Tetra, Tetrapol and DMR 34

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

4.1 Synthesis 34
4.2 Introduction..35
4.3 Performance 35
4.3.1 DMR 35
4.3.2 Tetrapol 36
4.3.3 Tetra 37
4.4 Geographical market 38
4.5 Norms and regulatory context 39
4.6 Level of security and threats 39
4.7 Main equipment manufacturers 40
4.8 Capital and operating expenditure..40
4.9 Which evolutions in the next five years..41
5 Short-range technologies.. 43
5.1 Synthesis 43
5.2 Introduction..43
5.3 Performances of short-range technologies..45
5.3.1 Bluetooth (802.15.1) 45
5.3.2 Zigbee (802.15.4)..46
5.3.3 Z-Wave..47
5.3.4 RFID/ NFC..49
5.3.5 Home RF 49
5.3.6 UWB..50
6 WiFi 51
6.1 Synthesis 51
6.2 Performance of WiFi systems 52
6.2.1 802.11a and 802.11b..53

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

6.2.2 802.11g ... 53
6.2.3 802.11n ... 53
6.2.4 802.11ac ... 54
6.2.5 802.11ad or WiGig ... 54
6.2.6 IEEE 802.11 at the era of 5G ... 55
6.2.7 WiFi in industrial environment ... 58
6.3 Geographical market ... 58
6.4 Norms and regulatory context ... 59
6.5 Level of security and threats ... 59
6.6 Main equipment manufacturers ... 59
6.7 Which evolutions in the next five years? ... 60
6.8 Maturity of the ecosystem in the years to come ... 60
7 WiMAX ... 61
7.1 Synthesis ... 61
7.2 Performances of WiMAX technology ... 61
8 Short-range industrial technologies ... 65
8.1 Synthesis ... 65
8.2 Performance of short-range industrial systems ... 66
8.2.1 Wireless HART and ISA100a ... 66
8.2.2 WISA (WSAN) ... 68
8.2.3 IEEE P1451.5 ... 70
8.2.4 Wireless Profibus ... 70
8.3 Geographical market ... 72
8.4 Norms and regulatory context ... 72
8.5 Level of security and threats ... 73
8.6 Main equipment manufacturers ... 73

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

8.7 Which evolutions in the next five years? 73

9 LPWA technologies 74

9.1 Synthesis 74

9.2 Performance of LPWA technologies 74

9.2.1 SigFox 78
9.2.2 LoRa 80
9.2.3 LoRa @ 2.4 GHz 81
9.2.4 Ingenu 83
9.2.5 Senaptic (Telensa) 84

10 Mesh network technologies 86

10.1 Synthesis 86

10.2 Performance of mesh network technologies 86

10.2.1 Structured mesh networks 87
10.2.2 Ad-hoc mesh networks 88
10.2.3 Benefits of mesh networks 88
10.2.4 Technical challenges in mesh networking 89

10.3 IEEE 802.11s: adding mesh capability to WiFi networks 90

11 Sources 92

12 Glossary 94

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figures

Figure 1: TRL evaluation scale 12
Figure 2: Throughput versus range 14
Figure 3: Maximum downlink throughput by type of mobile technology 18
Figure 4: Different specifications of LTE versions focused on IoT 25
Figure 5: Requirements of massive IoT networks and time-critical networks in the 5G specifications 26
Figure 6: The three main use case of 5G 31
Figure 7: 3GPP roadmap for 5G 32
Figure 8: DMR network architecture 35
Figure 9: TETRA architecture 38
Figure 10: Zigbee Alliance members involved in smart home 46
Figure 11: Z-Wave principle 48
Figure 12: Current protocols used per category of smart home devices 48
Figure 13: Difference with narrowband and Ultra wideband signal 50
Figure 14: Mobile-WiMAX architecture 63
Figure 15: HART installed base 68
Figure 16: WISA-WSAN timeline (1998-2012) 69
Figure 17: industrial communication market in 2015 71
Figure 18: ISM band allocation in various regions of the world 72
Figure 19: LPWA and wireless IoT technologies 75
Figure 20: Landscape of IoT/M2M networking technologies 76
Figure 21: LPWA technologies mapping of RF technologies in terms of range and consumption 77
Figure 22: SIGFOX coverage in Europe 80
Figure 23: Principle of LoRa 81
Figure 24 : Application of Ingenu for smart parking 84
Figure 25: Principle of Senaptic Ultra Narrow Band architecture 85
Figure 26: Schematic representation of a mesh network 87

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Tables

Table 1: Evaluation scale used in this report 11
Table 2: Summary of RF technology specifications (1/3) 13
Table 3: Summary of RF technology specifications (2/3) 15
Table 4: Summary of RF technology specifications (3/3) 16
Table 5: Commercial mobile network technologies – synthesis 17
Table 6: Presentation of main 2G technologies 19
Table 7: Mobile operators 2G shutdown plans 20
Table 8: Description of the main 3G technologies and their evolution 21
Table 9: Theoretical peak throughput in Mbps depending on spectrum, MIMO and modulation configurations with LTE-A 23
Table 10: Different specifications of LTE versions focused on IoT 25
Table 11: FDD and TDD most popular frequency bands for LTE 27
Table 12: IMT-2020 criterion for 5G (to be recognized as a 5G technology) 30
Table 13: PMR technologies – synthesis 34
Table 14: DMR specifications 36
Table 15: TETRAPOL specifications 37
Table 16: TETRA specifications 38
Table 17: PMR manufacturers 40
Table 18: Indicative cost elements for TETRA/TETRAPOL networks 41
Table 19: Presentation of selected TETRA networks in Europe 41
Table 20: Short-range technologies - synthesis 43
Table 21: Pros and cons of short-range technologies 44
Table 22: Features of main short-range technologies 45
Table 23: Bluetooth classes 45
Table 24: WiFi technology - synthesis 51
Table 25: WiFi generations 52
Table 26: WiMAX technology - synthesis 61
Table 27: Mobile WiMAX characteristics 62
Table 28: Mobile-WiMAX data rates 63
Table 29: Short-range industrial technologies - synthesis 65

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 30: WirelessHART characteristics 67
Table 31: WISA versus Bluetooth 70
Table 32: Maximum authorized distance depending on throughput 71
Table 33: Equipment manufacturers by industrial communication technology 73
Table 34: LPWA technologies - synthesis 74
Table 35: Characteristics of LPWA 75
Table 36: LPWA technologies comparison 78
Table 37: LoRa@2.4 GHz 82
Table 38: Mesh network technologies - synthesis 86

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

1 Structure and content of the report

1.1 Technologies covered in the report

- Commercial mobile network technologies: 2G, 3G, 4G and 5G
- Professional Mobile Radio technologies (PMR): Tetra, Tetrapol and DMR
- Short-range technologies:
  Bluetooth
  Zigbee
  Z-Wave
  RFID/NFC
  Home RF
  UWB
- WiFi
- WiMAX
- Short-range industrial technologies
  Wireless HART and ISA100a
  WISA (WSAN)
  IEEE P1451.5
  Wireless Profitbus
- LPWA technologies
  SigFox
  LoRa
  LoRa @ 2.4 GHz
  Ingenu
  Senaptic (Telensa)
- Mesh network technologies

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

1.2 Presentation of wireless technologies

For each technology analysed in this report, the following criteria and characteristics are detailed:

- Future role of these solutions in the industry/evolutions of the technology in 5 years
- Performances
- Geographical market
- Norms and regulatory context
- Level of security and threats
- Main equipment manufacturers
- Maturity level
- Stakes regarding market and competition
- Which evolution in the next five years?
- Maturity of the ecosystem in the years to come
- Main providers
- Price of equipment

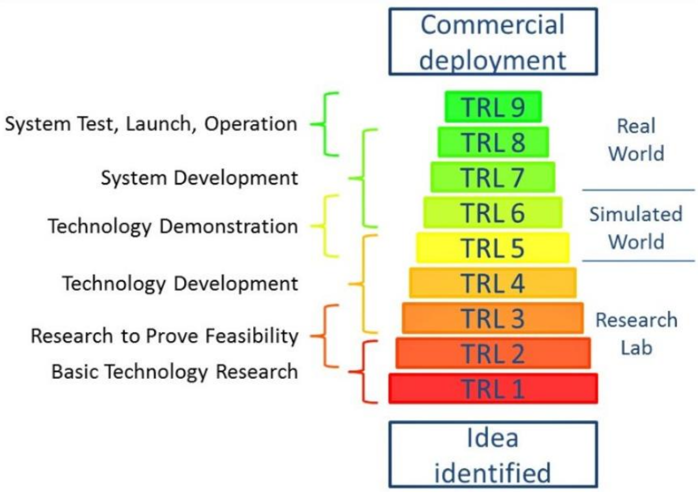
1.2.1 Performances & TRL evaluation scale used in this report

Table 1: Evaluation scale used in this report

Evaluation	Meaning
"-"	Below average
"+"	Fair
"++"	Good
"+++"	Very good

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 1: TRL evaluation scale



NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

2 Synthesis

The following tables summarize the main characteristics for each technology family studied in this report:

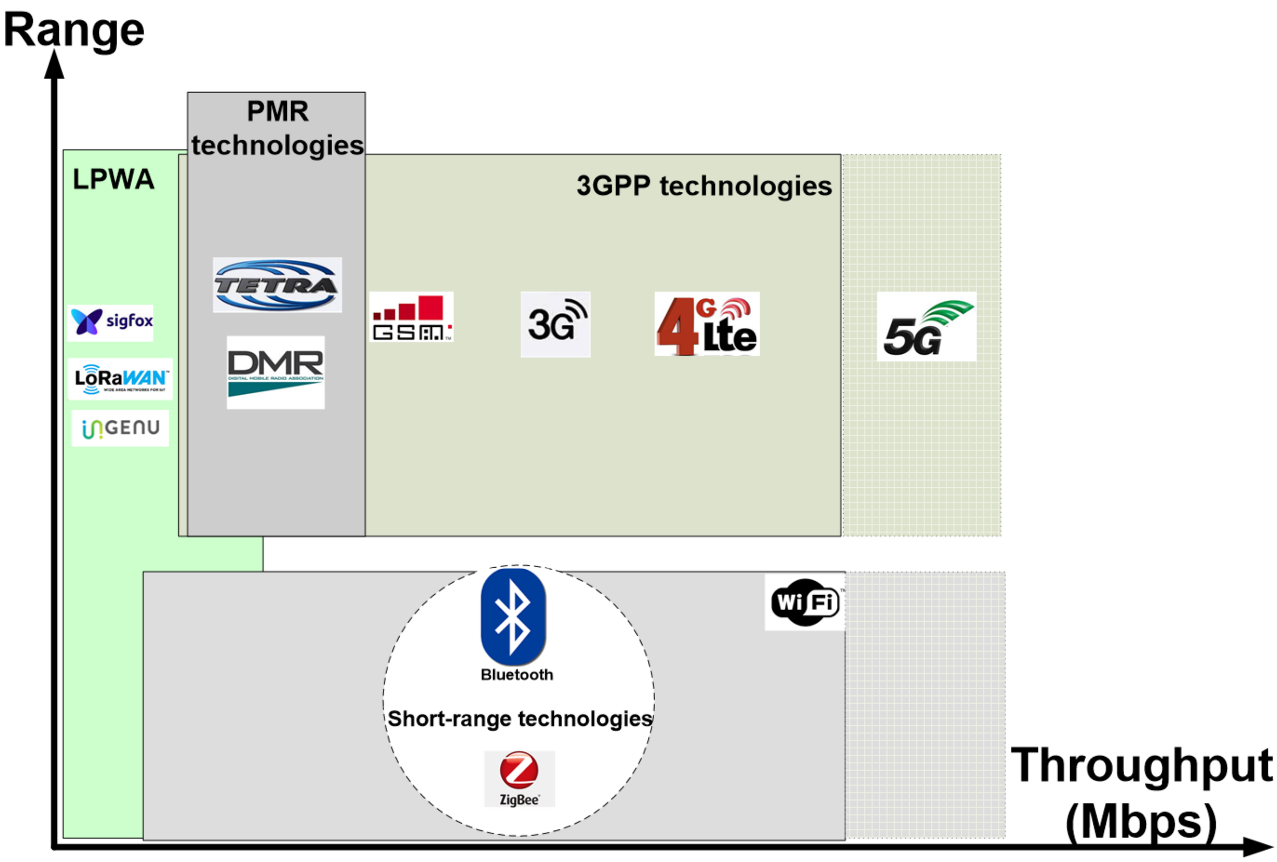
Table 2: Summary of RF technology specifications (1/3)

Technologies	Commercial mobile network	PMR	Short-range technologies	WiFi	WiMAX	Short-range industrial technologies	LPWA	LoRa @ 2.4 GHz	Mesh network technologies
Standards	3GPP (2G, 3G, 4G)	ETSI: Tetra, Tetrapol, DMR	Bluetooth, Zigbee, Z-Wave, RFID/NFC, Home RF, UWB	IEEE 802.11a, b, g, n, ac, ad, ah, ax, ay	IEEE 802.16 d,e	IEEE Wireless HART, WISA, IEEE P1451.5, IEC: Wireless Profitbus	Proprietary: SigFox, LoRa, Ingenu, Senaptic	Proprietary	IEEE 802.11s, 3GPP
Frequency band	From 600 MHz to 3.5 GHz (4G)	From 150 MHz to 2.6 GHz	868 MHz (EU), 915 MHz (US), 2.4 GHz	2.4 GHz 5 GHz	2.3 GHz 2.5 GHz 3.5 GHz	2.4 GHz	868 MHz (EU), 915 MHz (US), 470 MHz (CHN)	2.4 GHz	2.4 GHz
Interoperability	Yes	Yes	No	Yes	Yes	No	No	-	-
Battery life	1 day (smartphone), 10 years (M2M)	A few days	1 month to +years	A few hours	1 day (smartphone)	1 month to +years	10 to 20 years	Up to 5 years (1 msg per day)	A few hours
Bitrate	A few kbps to 1 Gbps	Max. 28 kbps	250 kbps	Up to a few Gbps	A few Mbps	9.6 kbps to 4 Mbps	100 bps - 50 kbps	270 kbps (UL & DL)	Up to a few Mbps
Mobility management	Yes	Yes	No	No	Yes (.e)	No	No	No	No
Two-way communications	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Range	Up to 30 km	Up to 50 km (TETRA)	20-100 m	Up to 200-300m	A few km	20-100 m	Up to 20 km	Up to 20 km (80 km?)	Short to long range (up to 20 km)
Footprint (geographical availbility)	Global	Global	Global	Global	Global	Global	~30 countries	Limited	Limited
Maturity (TRL)	9	9	9	9 (8 for ax and 6 for .ay)	9	9	9	8	9

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

The figure below shows range and throughputs for the different technology families:

Figure 2: Throughput versus range



Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

LPWA technologies technical characteristics are presented in the table below:

Table 3: Summary of RF technology specifications (2/3)

Technology	Cortus/ DASH7	LoRa	SigFox	Weightless-N	Weightless-P	Senaptic	Ingenu
Frequency band	433/868/915 MHz	868 MHz (EU) 915 MHz (US) 470 MHz (CHN)	868 MHz (EU) 915 MHz (US) 470 MHz (CHN)	868 MHz (EU) 915 MHz (US)	169/433/470/780/ 868/915/923 MHz	60/200/433/ 470/868/ 915 MHz	2.4 GHz
Interoperability	Standard	Proprietary	Proprietary	Standard	Standard	Proprietary	Proprietary
Battery life	20 years	+10 years	20 years	10 years	10 years	10 years	20 years
Bitrate	9.6 kbps	300 bps - 50 kbps	100 bps	100 bps	200 bps – 100 kbps	72.5 bps (UL)/500 bps (DL)	624 kbps (UL) / 156 kbps (DL) 2 kbps in mobility
Mobility management	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Two-way communications	Yes	Yes	Not really (kind of 2-way since mid-2015)	Yes/No	Yes	Yes/No option	Yes
Range	1-2 kms	15 km in rural 2-5 kms in dense areas	Up to 40 km in rural areas	3 km in urban	2 km in urban	20 km rural 3 km in urban	48 kms
Transmission through thick walls	+++	++	+	+	+	-	++
Footprint (geographical availbility)	Deployed ?	28 countries on 4 continents	29 countries mainly in Europe	3 cities	Deployed ?	30 countries	Global but mainly US

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Short-range technologies technical characteristics are presented in the table below:

Table 4: Summary of RF technology specifications (3/3)

Technology	ZigBee	Z-Wave	BLTE	Wi-Fi	UWB	Cellular (NB-IOT)
Frequency band	868 MHz (EU) 915 MHz (US) 2.4 GHz	868.42 MHz (EU) 908.42 MHz (US) Other	2.4 GHz	2.4/5GHz	3-10 GHz	LTE bands
Interoperability	Standard	Proprietary	Standard	Standard	Standard	Standard
Battery life	2 years	2 years	Months/years	Days	Months/years	10 years
Bitrate	250 kbps (from 20kbps for Zigbee GreenPower)	100 kbps	125 kpbs/500kbps/1 Mbps/2 Mbps	11-54 Mbps	480 Mbps- 2Gpbs	Tens of kbps
Mobility management	No	No	No	No	Yes	No
Two-way communications	Yes	Yes	Yes	Yes	Yes	Yes
Range	Hundreds meters	100m	>100m	300m	Few meters	10-15 km
Transmission through thick walls	+	++	-	+	-	--
Footprint (geographical availbility)	Global	Global	Global	Global	Deployed?	Global

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

3 Commercial mobile network technologies

3.1 Synthesis

Table 5: Commercial mobile network technologies – synthesis

Commercial mobile network technologies	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	+++ 4G is likely to be adopted for both unlicensed and licensed use in the factory of the future
Description	See detailed description below + References to external sources
Standards and regulatory constraints	3GPP
Area of operation	Worldwide
Protocols used	See detailed description below
Security	++
Performances	+++
Range	1 to 30 km depending on frequency band used and power level
Electrical consumption	Base stations: +++hundred Watts Devices: on battery (1 to 2 days for smartphones, many years for M2M 2G devices)
Environmental aspects (ATEX, gas, temperature, CEM…)	ATEX certified base station antennas, chipsets available
Use sectors (public networks, industrial networks, future use for FoF)	Public networks 5G for Industrial networks and FoF
Maturity (TRL)	TRL 9 for 2G, 3G and 4G 5G: TRL 5 to 7
Availability & associated constraints	Wide availability for network equipment and chipsets & devices
Main providers	Networks: Huawei, Ericsson, Nokia, ZTE, Samsung Devices: Samsung, Apple, Huawei…
Price of equipment	Base station: €50K to 100K Devices: €20 to 1000

Source: IDATE

3.2 Introduction

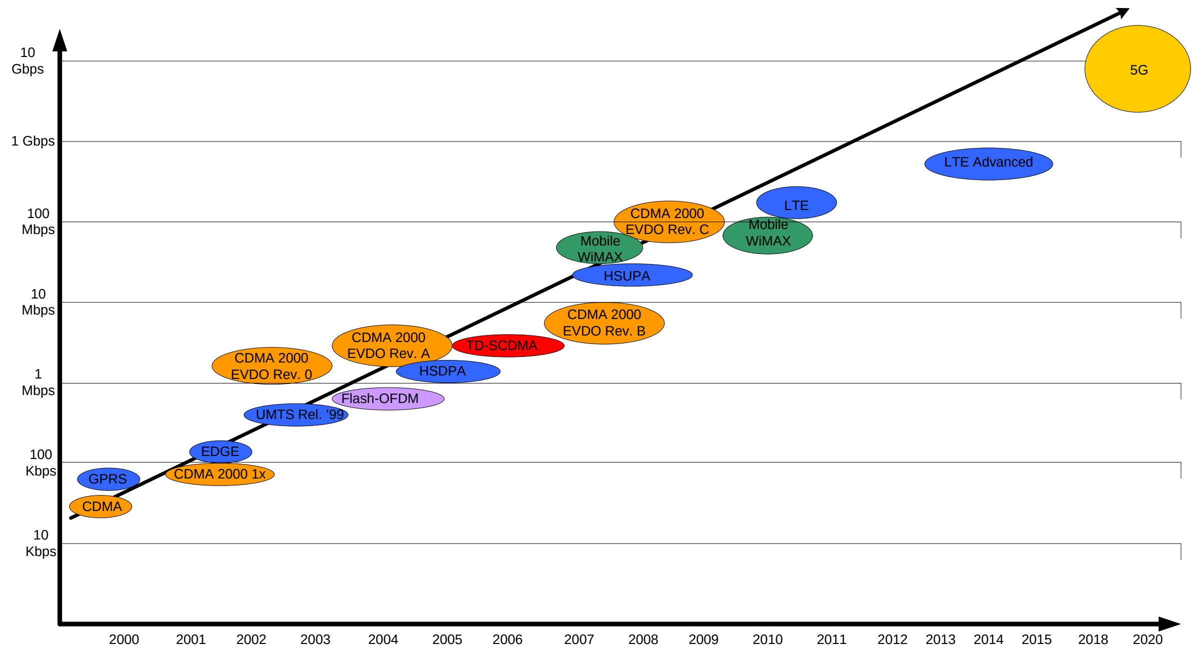
Commercial mobile network technologies are often considered through the generation of technologies they belong to. To simplify, those technologies are often referred to as 1G, 2G, 3G, 4G and so on. Those categories of technologies

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

include a set of technologies sharing the same technical capabilities. In the following sub parts, we will rapidly go through the 1st and 2nd generation of mobile technologies to focus more on 4G and the upcoming 5th generation mobile technology

It should be reminded that technologies are often incremental. Building blocks are improved little by little and separately before they are all gathered to produce the next generation technology for mobile communication. One radio component usually contains one antenna, filters, amplifiers, frequency converters, a modem and a battery. Innovation is permanent and can relate to any of those components, i.e. hardware components but also and it is more and more the case, to software elements.

Figure 3: Maximum downlink throughput by type of mobile technology



Source: IDATE

Mobile technology standardization processes freeze innovation at a given time but it doesn't guarantee that best technological blocks are systematically integrated in the standard. Standardization process eventually depends on the bargaining between the various parties at stake and result in choices that set the reference in the industry.

From this comes the fact that standardization process at the industrial level are essential in the definition of the next generation of mobile communication technology. Discussions that will be held will deal with several technological blocks and not only on one element that would enable to characterize on its own the future standard. Last but not

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

least, the incremental aspect of standardization process highlights the fact that a lot of elements that will be retained in the standardization process are already there in technologies already deployed on the ground.

3.3 Performance of commercial cellular technologies

3.3.1 1st generation (1G)

Technologies of first generation are analog technologies launched in the 70s in several parts of the world. Technologies such as NMT (Nordic Mobile Telephone), AMPS, TACS are all good examples of such technologies. Really Deployed at the beginning of the 80s, those networks have been rapidly replaced by 2nd generation technologies that were digital and more reliable. Hardly no 1st generation networks are today still commercially operated.

3.3.2 2nd generation (2G)

In this category, two families of technologies are usually identified: The GSM family was first supported by European people then largely adopted throughout the world while the CDMA technology was pushed by the US ecosystem. Its main difference was the use of a spread spectrum technology with special coding scheme as compared to the Time Division Multiple Access scheme that is used by GSM.

Each of those technologies have evolved to support the transmission of data in packet mode with GPRS and EDGE for GSM and CDMA1xRTT for CDMA.

Table 6: Presentation of main 2G technologies

GSM		CDMA One	
GPRS (2.5G)	Up to 50 Kbps (theoretical)	CDMA 1xRTT	Up to 153 kbps (theoretical)
EDGE (2.75G)	Up to 384 Kbps (Theoretical)		

Source: IDATE

Today, 2G technologies are still massively used throughout the world but some operators however have already shutdown or have planned to do so in the next 5 years. The table below shows operator plans regarding 2G shutdown in the world. Japanese operators were the first to switch off their 2G asset so as to release spectrum for 3G and 4G but other operators have followed, notably AT&T in the U.S and Australian operators. Generally speaking, however, 2G should remain in commercial operation for around 10 years still, although probably with reduced spectrum allocation

Interestingly, in some instances, operators will switch off 3G before 2G. One thing to consider indeed when shutting down 2G is that it is still used in M2M market in modules that often have a very long lifecycle. Furthermore, the very limited cost of 2G technology is still difficult to match by newer generation mobile technologies. This is the reason why specific low energy narrowband features have been recently developed for 4G. Sometimes, those 2G networks

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

will be kept under operation but infrastructure will be shared with other operators for that matter in order to limit the resources allocated to this otherwise aging technology.

Table 7: Mobile operators 2G shutdown plans

Countries	Operators	Information
Australia	**Telstra**	2G (GSM) terminated on December 1, 2016
	Optus	2G (GSM) terminated on April 1, 2017
	Vodafone	End of 2G (GSM) on September 30, 2017
Benelux	**T-Mobile (NL)**	2G shutdown in 2020
Canada	**Bell**	2G shutdown in January 1, 2017
	Telus	End of 2G in January 31, 2017
	Rogers	2G in early 2018
Japan	**NTT DoCoMo**	Service terminated on March 31, 2012
	SoftBank Mobile	Service terminated on March 31, 2010
	KDDI	au: Service terminated on March 31, 2003 TU-KA: Service terminated on March 31, 2008
New Zealand	**Telecom New Zealand**	2G sunset in July 31, 2012
Norway	**Telenor**	GSM switch off in 2025 (after 3G)
Singapour	**M1**	2G terminated in April 1, 2017
	Singtel	
	StarHub	
Switzerland	**Swisscom**	2G shutdown in December 31, 2020
Taiwan	**Chungwa Telecom**	2G shutdown scheluded for June 2017
	Far Eastone Telecom	
	Taiwan Mobile	
USA	**AT&T**	2G switch off in December 1, 2016
	T-Mobile	2G functional through to 2020
	Verizon	2G by the end 2019, 3G for 2021 ?

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

3.3.3 3rd generation (3G)

3rd generation mobile communication technologies are those recognized by ITU as matching criterion set by IMT-2000. The technical requirements specify that those technologies must enable throughput superior to 200 Kbps, something that sometimes set EDGE as a 3G technology. Practically however, it is considered that WCDMAX on one side and CDMA EV-DO rev A on the other side are the two 3G technologies. In October 2007, WiMAX, developed by the WiMAX Forum as port of the IEEE was also recognized as being part of IMT-2000 technologies and thus 3G.

Table 8: Description of the main 3G technologies and their evolution

	Mobile WiMAx	WCDMA	HSPA	HSPA+	DC-HSPA+	EV-DO RevA	EV-DO Rev B
Max throughput per sector (DL=downlink UL=uplink)	DL: 20 Mbps (canaux 14 MHz)	DL: 2 Mbps UL: 384 kbps	DL: 14,4 Mbps UL: 2 Mbps	DL: 21 Mbps UL: 5,76 Mbps	DL: 42 Mbps UL: 5,76 Mbps	DL: 3,1 Mbps UL: 1,8 Mbps	DL: 14,7 Mbps UL: 5,4 Mbps
Bandwidth	1,5-14MHz	2x5MHz	2x5 MHz	2x5 MHz	10 MHz (carrier aggregation)	1,25MHz	Carrier aggregation
Frequency bands	2.3-2.5-3.5 GHz	850-900 MHZ 1,5-1,7-1,9 GHz	850-900 MHZ 1,5-1,7-1,9 GHz	850-900 MHZ 1,5-1,7-1,9 GHz	850-900 MHZ 1,5-1,7-1,9 GHz	800 MHz-1,5-1,7-1,9-2,1GHz	800-1,5-1,7-1,9-2,1GHz
Multiplex mode	sOFDMA	TDMA, CDMA	TDMA, CDMA	TDMA, CDMA	TDMA, CDMA	CDMA	
Duplex mode	TDD/	FDD	FDD	FDD	FDD	FDD	FDD
Standard	IEEE 802.16-2005	3GPP	3GPP	3GPP	3GPP	3GPP2	3GPP2

Source: IDATE

In France, GSM technologies and work from the 3GPP have a dominant place in the telecommunication landscape, something that is largely shared with other European countries. Developed by the American, CDMA and its evolution are hardly used in Europe to the exception of some eastern countries where the technology was notably used in the 450 MHz to cover very larger but scarcely populated areas. In the year 2005, WIMAX technology however appeared in the landscape as a very promising technology to be used to provide mobile broadband services. In France however, the technology was seen by public authorities as dedicated to the providing of fixed broadband in grey areas, therefore limiting its use to the 3.5 GHz band. This band is not propitious for large coverage and was restricted to nomadic use at best and associated to regional only licenses.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

After the failure of the development of the Wireless Local Loop in the years 2000, WIMAX indeed appeared as a mature technology capable of supporting multiple Mbps without line of sight, something that was much looked for grey areas. Technologically in advance over other legacy 3GPP technologies WIMAX however suffered from a lack of industrial support and the hardware ecosystem failed to develop, to the extent that no WIMAX carrier in France eventually deployed the number of site that their license legally required.

It is to be said nonetheless that WIMAX technology was deployed on large scale abroad for fixed as well as mobile usage. In Japan, KDDI was notably known for its WIMAX network deployed by its sister company UQ Communication reaching 4.1 million subscribers by the end of 2015. Since then the technology has evolved to become compatible in its WIMAX 2 version with TD-LTE, one flavor of 4th Generation technology LTE.

3.3.4 4th generation (4G)

Although often called 4th generation technologies, WIMAX and LTE did not satisfy with ITU criterion defined for IMT-Advanced when they were launched. Indeed, those technologies were to be able to provide 1 Gbps throughput in stationary situation and 100 Mbps when in mobility, something that is only starting to be possible with the Release 13 of LTE. In December 2010, however, ITU decided to recognize to call those technologies 4G technologies, noting the significant advances they had brought as compared to 3G at the beginning.

The main criterions to satisfy the definition of 4G are:

- To be an All-IP technology (which mean no circuit mode for voice)
- Enable a 100 Mbps throughput in mobility and 1 Gbps when stationary
- Being able to flexibly use a bandwidth between 5 and 20 MHz
- Provide a spectral efficiency of 15 bit/Hz in the downlink and 6.75 bits/ Hz in the uplink
- Offer Quality of Service

Today, two technologies satisfy those criterions and can truly be considered as 4th generation technologies. Those are LTE-A or Long Term Evolution Advanced and IEEE 802.16m or WIMAX Advanced. This latter technology actually provides a convergence toward TD-LTE with which it is compatible. In many respects, IEEE 802.11m is the ultimate evolution for WIMAX players enabling them to softly migrate toward LTE (LTE-A) technology, which is supported and adopted by a large majority of carriers worldwide.

As we mentioned earlier, under an apparently unified branding, a technology is actually a set of multiple technologies. LTE-Advanced is a telling example in this regard. When we mention the capability of such or such technology to reach such or such throughput, we have to take into account which features are required to satisfy this level of performance.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

With LTE-A, but this is often the case with other technologies, several characteristics influence the final performance:

- The amount of spectrum that can be leveraged. With LTE and LTE-A, one carrier can be as large as 20 MHz. With LTE-A (starting with 3GPP LTE Rel 10), several carrier components of up to 20 MHz can be aggregated.
- The modulation used and its efficiency. While early releases of LTE supported the use of up to 64QAM, Release 12 of LTE brought the support of 256QAM modulation enabling to transport 33% more bits per signal than 64 QAM, effectively increasing throughputs by the same 33% with the same bandwidth used. The more complex and efficient the modulation the better the strength of the signal is required. This means that 256 QAM will be available only to the users the closest to the antenna
- The number of antenna used: By default, 2x2 MIMO is supported by LTE but up to 8X8 MIMO was early on foreseen in the standard. Supporting such number of antennas in a device is however challenging from a processing power and battery life prospective. Today, most smartphone are in 2X2 MIMO configurations but first 4X4 MIMO devices have been launched in 2016 enabling to provide twice as much throughput for the same amount of spectrum.

Eventually, the performance of the network will thus be defined by those features. The table below highlights what kind of performance can be achieved depending on those parameters.

Table 9: Theoretical peak throughput in Mbps depending on spectrum, MIMO and modulation configurations with LTE-A

FDD	MIMO 2X2				MIMO 4X4				MIMO 8X8			
CA of 20 MHZ	QPSK	16 QAM	64 QAM	256 QAM	QPSK	16 QAM	64 QAM	256 QAM	QPSK	16 QAM	64 QAM	256 QAM
5x20	250	500	750	1000	500	1000	1500	2000	1000	2000	3000	4000
4x20	200	400	600	800	400	800	1200	1600	800	1600	2400	3200
3x20	150	300	450	600	300	600	900	1200	600	1200	1800	2400
2x20	100	200	300	400	200	400	600	800	400	800	1200	1600
1x20	50	100	150	200	100	200	300	400	200	400	600	800

Source: IDATE

What this table shows is that the same peak throughput can be reached in different ways. 300 Mbps downlink throughput for instance can be reached by aggregating 2 Carrier Component of 20 MHz with 64 QAM modulations and a 2x2 MIMO configuration. Similarly, it could be reached with only 20 MHz of spectrum and 64QAM but a 4x4 MIMO configuration both at cell site and in the device.

It is also to be understood that there is a discrepancy between what the standard foresee and enable and the real availability of commercial equipment capable of supporting such feature. As an example, 3GPP LTE Rel 13 theoretically enables to aggregate up to 32 Carrier Component of 20 MHz. Operators however do not have such spectrum assets today and implementing the aggregation of 32 CC of 20 MHz raises significant challenge, which do not make it practical as of today for commercial usage.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

As of end of July 2017, the fastest LTE network available support Gigabit speeds in the downlink thanks to the combination of 4x4 MIMO, 256 QAM and the aggregation of 3 or 4 Carrier Component of 20 MHz. Telstra in Australia was the first operator to launch such capability on its commercial network back in February 2017 but other operators such as Sprint in the US have followed and other operators will follow as more devices are launched on the market.

3.3.5 The case for cellular IoT

In order to better address low power applications, the 3GPP workgroup published Release 12 and Release 13 where it planned to study the "provision of low-cost Machine-Type Communication UEs based on LTE".

It aims to look at new features to allow the manufacturing of low-cost and low-consumption M2M devices. Indeed, the main issue with M2M LTE devices is cost. Still, LTE module prices have already declined significantly to as little as 80 USD in the US (where LTE is already rolled out). The goal is to provide LTE-M module cost close to GPRS module cost.

The Machine-Type Communications (MTC) can be split into two approaches:

- MTC over 2G refers to the various approaches using 2G (GSM) infrastructure. The most prominent of them is the Neul-Huawei Clean Slate, but other companies such as Qualcomm and Ericson have submitted proposals as well. The leading module manufacturer Sierra Wireless is also pushing **EC-GSM**. The 2G proposals repurpose a single 200 kHz GSM voice channel into multiple MTC channels. Given the existence of infrastructure and the additional link budget proposed, enhanced coverage could be achievable. However, sustainability of the 2G/2.5 spectrum is a major concern worldwide. Several 2G licences will expire by 2021-2022. AT&T has already announced it will shut its 2G network down in the US by 2017. On its customer perspectives, the cost of the obsolete 2G modules substitution is very high and has obviously a negative impact on the customer relationship.
- MTC over LTE is the forward path, which attempts to allow the MTC devices on 4G LTE spectrum with some optimisations to help coverage, cost, and battery life. These proposals are backed by the main equipment vendors in the mobile industry: Qualcomm, Huawei, Ericsson, Samsung and others. However, the cost of scaling the cellular network for deep coverage is still expected to be prohibitively expensive. The idea is to meet M2M requirements in terms of throughput and underlying low power consumption. Among LTE-based solutions, different versions exist including **LTE Cat 0, LTE-M** and in the late summer of 2015, a group composed of Ericsson, Intel and Nokia announced plans to throw their weight behind a new specification called Narrow-Band Long-Term Evolution (NB-LTE, renamed **NB-IoT**). Moreover, even though LTE spectrum seems to be the forward path, the network longevity also depends on the rate at which cellular technology advances without backward compatibility.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 10: Different specifications of LTE versions focused on IoT

	EC-GPRS	LTE- 0	CAT-M1 (LTE-M)	CAT-NB1 (NB-IOT)
Frequency bands	900-1800 Mhz	LTE (20 MHz)	LTE (1 MHz)	LTE (200 KHz)
Range	20 dB improved compared to GPRS	10-15 km	10-15 km	10-15 km
Bidirectional	Yes	Yes	Yes	Yes
Datarate	GPRS (56–114 kbps)	Up to 1Mbps	From tens of kbps to 1Mbps	Up to tens of kbps
Mobility support	Yes	Yes	Yes	No
Power consumption	Low	Low	Low	Low
Frequency bands	900-1800 Mhz	LTE (20 MHz)	LTE (1 MHz)	LTE (200 KHz)

Source: IDATE DigiWorld, *The Industrial Internet*, May 2017

Telcos already position themselves on those MTC versions such as US telcos AT&T and Verizon and KT on LTE-M. Others - Telecom Italia, China Mobile, China Telecom, China Unicom, Etisalat, Telefónica, LG U+, Orange - selected NB-IoT and Vodafone launched the first commercial trial in Madrid in September 2016.

Figure 4: Different specifications of LTE versions focused on IoT

Attribute	CAT-M1	CAT-NB1	EC-GSM
Spectrum	LTE bands	LTE and Refarmed 2G Bands	2G Bands
Typical MNO	Good LTE Coverage	Mix LTE and 2G	Long 2G Life
Data Rate	375kbps	20-65kbps	70 kbps
Channel BW	1.08MHz	200KHz	200KHz
Mobility	Yes	No	Yes
Specification Available	Now 3GPP	Q2'16	Now 3GPP
IP vs messaging	Both	Simple message or very low data	Both
Voice Capable	Yes	No	Yes
Network Roll Out	S/W Upgrade	S/W Upgrade	Mostly S/W Upgrade
Public Network Availability	Q1-Q2'2017 NA, Aus., Japan, EU	Q1-Q2'2017 EU,China,NA	Q4'2016 EU

Source: Sierra Wireless

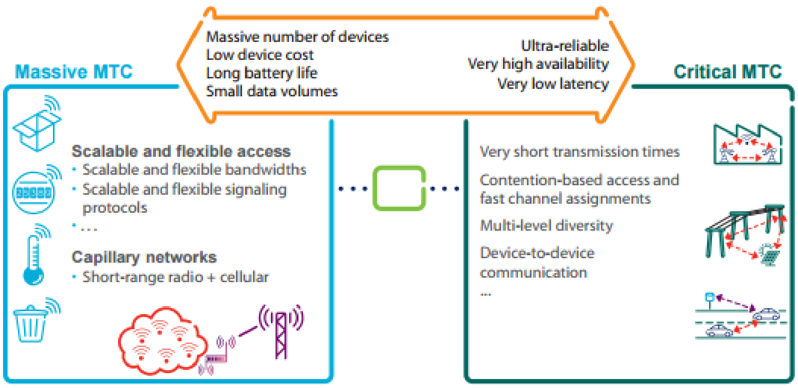
NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

In parallel, all operators are working on the integration of IoT in the 5G umbrella. Unlike 4G, 5G will be standardised from the outset, taking into account the constraints of the Internet of Things. Indeed, in addition to faster mobile broadband (enhanced 4G bitrate), 5G design will integrate requirements of major IoT applications. Leading vertical industrials are involved from the beginning of the 5G standardisation process.

Even though the scope of 5G is still not definite, standardisation allows for two types of IoT-focused services:

- **Massive MTC** where the key challenge is to meet the volume issue: the network has to be designed to handle the traffic of tens of billions of objects. This category will affect most IoT applications, notably the remote reading of energy meter sensors, management of parking and waste management.
- **Critical MTC** where QoS issues are very important. This category will concern applications dealing with real human risks, principally the autonomous car, predictive maintenance of aircraft engines and management of traffic lights.

Figure 5: Requirements of massive IoT networks and time-critical networks in the 5G specifications



Source: Ericsson

3.4 Geographical market

While GSM, UMTS and LTE can be found all over the world, CDMA based network are less popular especially in Europe where GSM is largely dominant. As a result, from 3GPP2 being an association between ARIB (Japan), CCSA (China), TIA (North America) and TTA (South Korea), CDMA networks can be found in those countries and other countries with influence from those players. Latin America was notably a zone of influence for CDMA, and so was India.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

In Europe some CDMA networks can be found in eastern countries, notably because of its capability to be operate in the 450 MHz frequency bands.

3.5 Norms and regulatory context

LTE and 5G are currently developed by the 3GPP, an organization gathering several telecommunication players and created in 1998 to develop a 3rd generation mobile technology based on the European standard GSM. It is not to be confused with the 3GPP2 association which was created the same year with the aim of developing a 3G standard based on the American 2G standard called CDMA.

Later on, 3GPP developed its own technological proposition for a 4G standard and is since continuing its effort with 5G, which is, as of August 2017 the only candidate technology for IMT-2020. Because of the large support of the industry for LTE technology proposal, 3GPP2 did not propose competing technology. Qualcomm had a proposition with UMB but decided to halt its development in face of LTE large support.

LTE technology can currently be operated in more than 40 different frequency bands including the 5 GHz unlicensed band since LTE Release 13 and the specific 3.5 GHz CBRS band in the US. Main LTE frequency bands are presented below, they include 2G and 3G frequency bands, which can be refarmed for 4G operation.

Most popular frequency bands used by LTE networks are presented in the table below:

Table 11: FDD and TDD most popular frequency bands for LTE

(in terms of number of networks launched)

FDD band	Frequency	Comment
3	1800 MHz	Original 2G band
7	2600 MHz	4G Capacity band
1	2100 MHz	Original 3G band
20	800 MHz	Digital Dividend

Source: IDATE, GSACOM and 3GPP

TDD band	Frequency
40	2300 MHz
38	2600 MHz
41	2600 MHz
39	1900 MHz

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

The FDD mode is the most popular duplex division mode used with only 13% of LTE network launched operating in TDD mode. China Mobile is the largest TD-LTE operator but in the future, TDD mode should continue to grow, especially as higher and higher spectrum is being used. TDD mode is indeed better suited for asymmetric usage contrary to FDD mode which was ideally suited for symmetric usage such as circuit switched telephony

In the future, higher frequency bands (above 3 GHz up to 100 GHz in a more distant future) will be used to provide both increased capacity and individual throughputs. For operators with limited access to spectrum, it will be possible to leverage unlicensed spectrum with Licensed Assisted Access (LAA). This feature enables to use the unlicensed 5 GHz frequency band as a Supplemental Downlink to a licensed frequency band. In a latter release of LTE, it will also be possible to use unlicensed frequency band as Stand Alone.

As of today, LAA will be of great help for operators with limited licensed spectrum to launch LTE gigabit service. 5 GHz frequency band is standardized as band 252 and 255 under 3GPP in FDD Downlink only mode and as band 46 for TDD mode.

3.6 Level of security and threats

The level of security has kept increasing with each next generation of mobile communication technology, however, even 4G LTE has proven to be hackable. In 2015 for instance, an attack on a LTE network was demonstrated by a firm specialized in security. In order to do that, the company leveraged security flaws found in Diameter signaling protocol. It was thus possible to compromise the core network and possibly

- Interrupt 4G services
- Intercept signaling message and thus identify and locate subscribers roaming on the network

According to the company, this security flaw largely depended on ill configured and secured server, something that is easily possible to fix.

Another attack that was demonstrated consisted in forcing a 4G device to switch back to a rogue 2G base station where communications could be easily spied. This attack was revealed in October 2016 at a hacking convention in Melbourne, Australia. In order to fix this issue, 3GPP suggested strengthening security by rejecting one-way authentication and by rejecting requests of base station for weakened cyphering.

3.7 Main equipment manufacturers

Over the years, the cellular equipment manufacturer market has consolidated itself under the competitive pressure notably of rising Chinese players such as Huawei notably but also ZTE.

Main equipment manufacturers today are:

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

- Huawei
- Ericsson
- Nokia (purchase of Alcatel Lucent)
- ZTE
- Samsung

3.8 Maturity level

2G, 3G and 4G have a Technology Readiness Level of 9 which is the highest possible level. 5G on the other hand, which is still in development but for which trials and demonstration have already started, would have a TRL comprised between 5 and 7.

3.9 Stakes regarding market and competition

Today, LTE technology developed by the 3GPP has gained significant momentum around the world and is largely dominant in the mobile industry to such an extent that even competing WIMAX technology is now converging toward TD-LTE to offer a transition path to operators with WIMAX assets. It benefits from a wide ecosystem of more than 8,000 different devices operating on more than 40 different frequency bands, something that is much different from 3G, which was limited to 16 bands, even though two of them largely dominated over the other in terms of use.

Thanks to this wide ecosystem and support, LTE and its evolution LTE-Advanced and LTE Advanced Pro can be considered as a very mature technology with a very good evolution path toward 5G. Currently, LTE technology is little adopted in specific areas where proprietary and often older technologies are being used:

- Critical applications have historically relied on proprietary technologies and private networks, two areas where LTE and its evolutions was not originally positioned for. With LTE Rel 12 and 13 however, critical features where developed for LTE to support application such as Mission Critical Push To Talk, Device to Device communication, capability to handle call locally in case of network outage… With those added features, LTE and later on 5G are well positioned to become the transition path for a host of mission critical networks (e.g. Public Safety…), even though this kind of transition will last for many years;
- Low energy / low cost narrowband communication: Because of its focus on broadband and its relatively complexity, LTE raised both power consumption and cost challenges for certain kind of applications such as M2M. This is the reason for the development of new UE Categories for LTE to support lower energy lower cost application NB-IoT and LTE-M. In the meantime, other greenfield technologies outside 3GPP have been developed.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

3.10 Which evolution in the next five years

In the next five years, LTE-Advanced is set to continue its evolution toward 5G, which is also being standardized by 3GPP. Actually several features developed in latest 3GPP LTE releases will be part of 5G a technology that is really to be understood as a logical evolution of 4G to embrace even more diverse use cases and requirements. The performance requirements set by the ITU for 5G are presented below:

Table 12: IMT-2020 criterion for 5G (to be recognized as a 5G technology)

Criteria	Target value
Peak speed	Multiple Gbps
Average speed	100 Mbps (DL) and 50 Mbps (UL)
Spectral efficiency	30 bit per Hz (DL) and 15 bits per Hz (UL)
Increased capacity	At least 20 Gbps per cell (IMT-2020 requirement
Peak latency	1 ms

Source: ITU

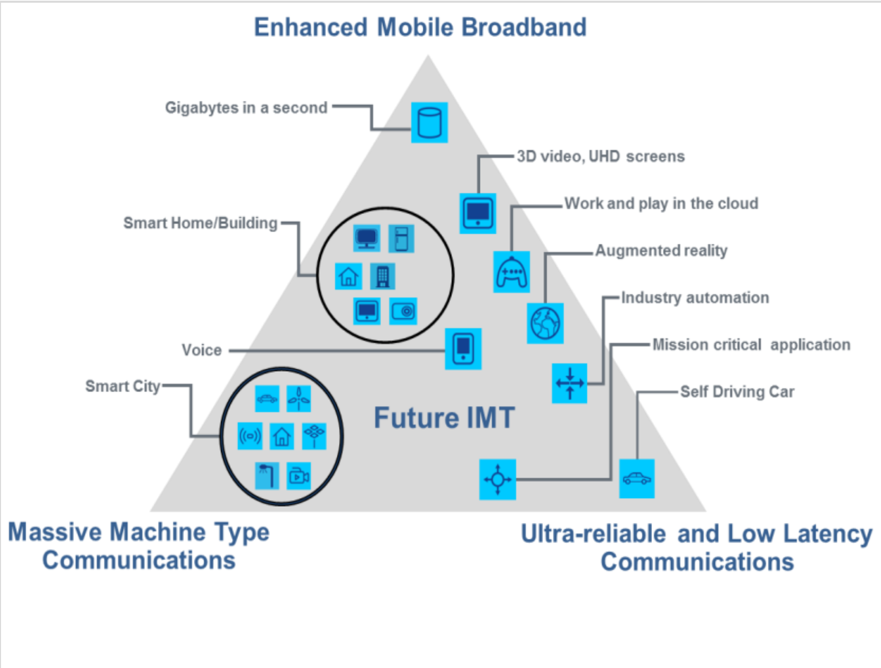
Some features and principle currently developed in current LTE Releases will be funding blocks of 5G

- Use of unlicensed spectrum, something brought by LTE-U and Licensed Assisted Access in Rel 13 and later. In 5G, other unlicensed frequency band will likely be considered such as the 60 GHz band. Other mode of access to the spectrum such as the multiple-tiered Spectrum Access System will be developed enabling even more flexible access to spectrum
- Massive MIMO: while LTE introduced Multiple Input Multiple Output in cellular networks, the number of antennas used will increase to configuration such as 64x64 MIMO systems at the cell site, something that has been studied as part of Rel 13. This type of MIMO configuration, in association with the use of higher frequency bands and more directive beams will drastically increase capacity at cell-site. 5G could use even more antenna elements
- Increased Quality of Service: While LTE brought some basic level of Quality of service, 5G will push the concept even further enabling services with sometime opposed requirements to run completely independently on the same infrastructure thanks to a concept called Network Slicing. It leverages Software Defined Network and Network Function Virtualization to allocate resources from different layers independently to each service
- Support for a denser network with more small cells in addition to broadcast and Device to Device communication. Those features have been lately available but will be further and more systematically used to depart from the typical Core Network / Macro cell architecture

At the same time, 5G will also differentiate itself from previous LTE Releases by putting the stress on flexibility and the support of multiple use cases rather than only the Mobile Broadband use case, which has been the focus of LTE. Three main use cases will be supported:

- enhanced Mobile Broadband, massive (eMBB)
- massive Machine Type Communication (mMTC)
- Ultra-reliable and low latency Communication (critical MTC)

Figure 6: The three main use case of 5G



Source: ITU-R

The flexibility required to support those main use cases will leverage on pre-existing technologies found in latest LTE Releases but also on completely new technologies and most importantly on a new architecture based on Network Slicing and other concept:

- The support for an increased range of spectrum, notably with the support of frequencies above 6 GHz and notably the mmWave bands where larger bandwidth will be possible. The basic bandwidth in those frequency range will be of 100 MHz (as compared to between 1.4 and 20 MHz for LTE)
- New Air Interface: Supporting new use cases in new operating conditions (higher frequencies, increased mobility, and increased battery life requirement) require a new air interface. While initially supporting 4G air interface at launch, a new more flexible air interface will be added.

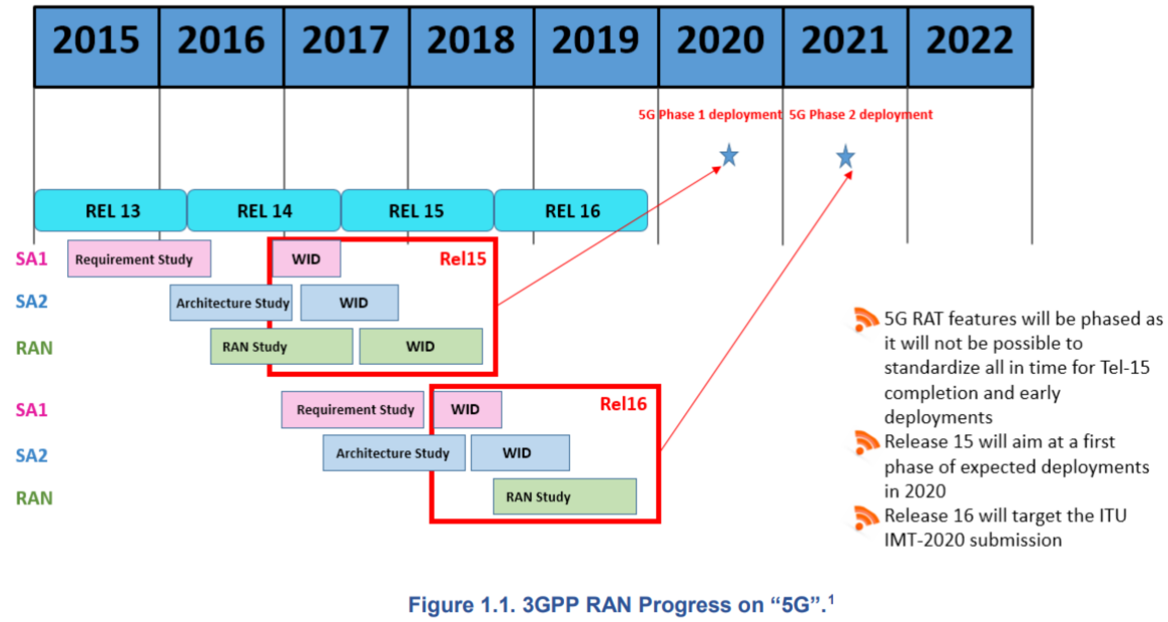
NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

3.11 Maturity of the ecosystem in the years to come

As of today, the 2G, 3G, 4G ecosystem can be considered as very mature with a wide range of equipment both for the infrastructure and the terminal side with interoperability between equipment a reality. Thanks to the wide support behind 5G in the industry, the situation should not be different with 5G but as with new Radio Access Network technologies, the 5G ecosystem should be limited at the outset. First 5G devices will likely be devices such as dongle and fixed CPEs with a limited number of 5G frequency bands supported and likely a certain device fragmentation depending on the geographical market. Initially, C band (3.4-3.8 GHz) and the 28 GHz (in the U.S. and South Korea notably) will be the two main frequency bands

First 5G baseband have already been presented but are not yet commercially available. Qualcomm has announced that its x50 5G modem will be available in 2018 for the first 5G trials and Intel plans to have its own baseband commercially available during the 1st half of 2018. First 5G commercial device could thus be launched in 2018 but the end-user device ecosystem should not start its real development before 2020-2021 when the standard will have been finalized.

Figure 7: 3GPP roadmap for 5G



Source: 3GPP

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Étude Bibliographique

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

4 Professional Mobile Radio technologies (PMR): Tetra, Tetrapol and DMR

4.1 Synthesis

Table 13: PMR technologies – synthesis

PMR	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	++ PMR systems are currently used in the industry but evolution to broadband communications will only be possible with 4G, not with an evolution of the existing PMR technologies
Description	Use for critical application for voice and messaging in the public safety and in private network
Standards and regulatory constraints	ETSI for TETRA, DMR and TETRAPOL
Area of operation	Worldwide (limited development so far in the US but good perspectives for the years to come
Protocols used	See detailed description below
Security	+++ (but possibilities for attacks exist nonetheless)
Performances	Data: limited to a few kbps
Range	400m in Direct Mode Operation (DMO) in urban environment, up to 2 km in rural areas Possibility to extend coverage through relay mode Up to 50 km (TETRA)
Electrical consumption	700W required for 25W of output power per carrier
Environmental aspects (ATEX, gas, temperature, CEM…)	Several implementations of equipment comply with ATEX directive (e.g. TetraFlex base stations from DAMM). Motorola provides ATEX certified DMR handsets
Use sectors (public networks, industrial networks, future use for FoF)	Public safety, private networks
Maturity (TRL)	TRL 9
Availability & associated constraints	Limited but real availability (as compared to commercial markets)
Main providers	EADS, Siemens, Motorola, Sepura, Teltronic, Rohill, Selex Communications, Rohde & Schwarz, Artevea, Damm, Sungard, Aselsan, Harris, Hytera, Kirisun, Radio Activity srl, Radio Data, Simoco, Tait communication , YaesuDevices: Samsung, Apple, Huawei
Price of equipment	Tetra base station: €30K, DMR base station: €5K Handset: ~€200-800

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

4.2 Introduction

Professional Mobile Radio technologies differentiate themselves from traditional GSM by providing additional and required voice features such as faster call set-up, group calls, priority calls, encryption, and ability to make direct calls without connection via a base station. This is the reason why markets with needs to support critical communication have relied on those technologies rather than traditional 2G, 3G and 4G.

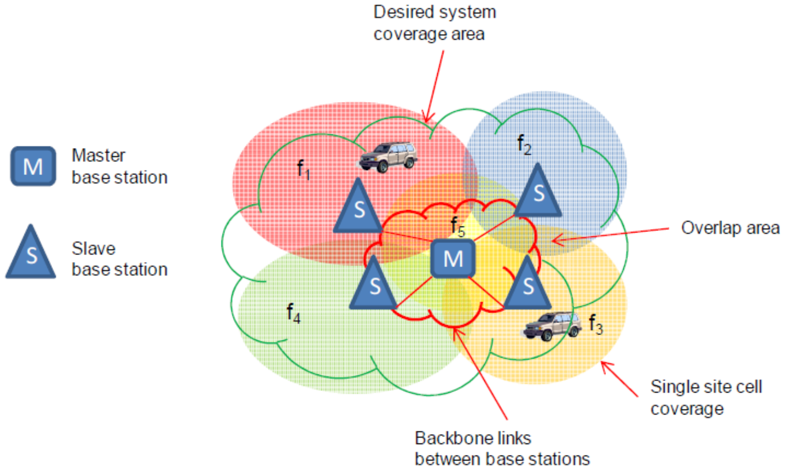
With 4G however and to a bigger extent with 5G, those features are now supported, which might make from both LTE-A latest releases or 5G a transition path for those users. This transition could be very long as many PMR networks are still analog.

4.3 Performance

4.3.1 DMR

Digital Mobile Radio is an open digital standard defined in an ETSI standard and used in commercial products all around the world. Designed and ratified lately (in 2005), the standard is aimed at overcoming the drawbacks of proprietary technologies where users are often stuck with the same infrastructure/terminal vendor because of interoperability issues and providing an easy transition path for all users still with analogue PMR technologies. DMR was thus devised as a low complexity, low cost and interoperable technology. In practice however, equipment manufacturers have introduced features that make each implementation of DMR not so interoperable.

Figure 8: DMR network architecture



Source: Radio Activity

DMR was designed with three different level of use and associated tier:

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

- Tier 1 is for use on the unlicensed band 446 MHz. This band however is not unlicensed in the U.S. where it is used by the US government and by radio amateurs, which has caused some issues in the country. It is designed to work without infrastructure other than relay
- Tier 2 is for use in Licensed bands between 66 and 960 MHz. It adds IP data services for high power communication
- Tier 3 adds trunking operation in licensed bands, supporting voice and short message handling. It notably supports IPv4 and IPv6 for packet data services. Tier III DMR devices were introduced for the first time in 2012. This latest tier is aimed at public safety and mission critical applications

DMR benefit from a relatively sizeable industrial ecosystem but as we mentioned, interoperability is not always secured because of the introduction by some manufacturers of proprietary features. The Simulcast process enables the use of the same frequency for all relays of a subdivision interconnected with IP microwave links.

Table 14: DMR specifications

DMR	Characteristics
Frequency bands	Between 66 and 990 MHz including unlicensed 446 MHz
Channel spacing	12.5 KHz
Number of channels by carrier	2
Access Mode	TDMA
Transmission type	Digital
Modulation	4 state FSK
Data Throughputs	2 Kbps per time slot
Voice coding	AMBE, 6 Kbps

Source IDATE

4.3.2 Tetrapol

TETRAPOL is a digital private network technology developed by Matra Nortel and based on Frequency-division multiplexing (FDMA) with narrow channels of 12.5 KHz. This technology enables to connect several different organizations together and is thus interoperable at the border with other national networks.

Standardized as soon as in 1988 as part of the designing and deployment of the first big digital PMR network in Europe for the French Gendarmerie Nationale, TETRAPOL was quite successful in France, Europe and in other parts of the world more specifically on the public safety, civilian or military market but also on the corporate market in industries such as transportation, logistic and automotive.

Operating on the 400 MHz frequency band, it is using a single Frequency division multiplexing without Time Division Multiplexing contrary to TETRA and GSM.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

It is accepted as a de facto standard at the international level by organizations such as ITU and CEPT and was designed to provide wide coverage. To promote the technology, notably against its competitor such as TETRA technology, a dedicated Forum was created in 1996. It is the organization that is in charge of developing the standard.

Table 15: TETRAPOL specifications

TETRAPOL	Characteristics
Frequency bands	Between 70 and 520 MHz (theoretically) but most popular bands are in the 80, 160 and 400 MHz
Channel spacing	10 KHz, 12.5 KHz or 6.25 KHz
Number of channels by carrier	1 channel by carrierpar porteuse
Access Mode	FDMA
Transmission type	Digital
Modulation	GMSK
Data Throughputs	8 Kbps
Voice coding	RPCELP, 6 Kbps
Coverage	On average the cell has a 100 km diameter
Capacity	Around 100 voice users by channel, one base station supporting between 4 to 16 channel in total

Source IDATE

4.3.3 Tetra

TETRA was developed in the framework of ETSI as a result of an initiative of PMR players such as Nokia, Motorola, Marconi. This standard mainly developed itself in Europe starting in 1996 but was never adopted in the U.S.

Its main technical characteristics positioned the technology as an interesting alternative to GSM in a professional (and demanding) environment with similarities but also notable differences: On one side, the frequency band used is in the 400 MHz, and on the other side the system works with Time Division Multiplexing (TDMA) with 4 users sharing the same frequency. This results in signals being pulsed with a frequency different form the GSM (17.6 Hz vs 217 Hz).

Although designed to compete with GSM, TETRA was never capable of reaching mass market, its main characteristics giving the technology an edge on certain niche market where security is involved (Police or Public Safety).

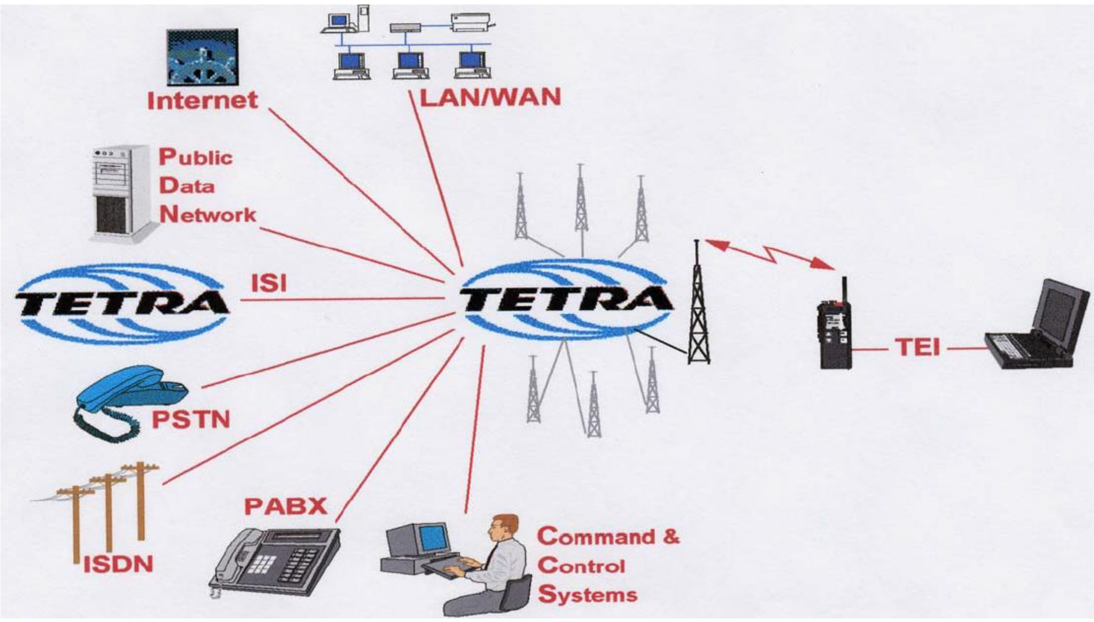
NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 16: TETRA specifications

TETRA	Characteristics
Frequency bands	380 to 400 MHz (and other bands)
Channel spacing	25 KHz
Number of channels by carrier	4
Access mode	TDMA
Transmission type	Digital
Modulation	4 DQPSK
Data throughputs	Max. : 28 Kbps
Voice coding	ACELP, 4.8 Kbps

Source IDATE

Figure 9: TETRA architecture



Source: TETRA Forum

4.4 Geographical market

The geographical market varies vastly depending on the technology considered. While it is considered that TETRAPOL only account for a fraction of the total market with TETRA having the largest share of the pie worldwide if we exclude

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

analog, TETRAPOL is still used all over the world in 80 networks in 34 different countries. In Europe, which is its main market, TETRAPOL used to claim 70% of the European Digital Public Mobile Radio market but TETRA technology has since then made much progress and, according to HIS accounted for 53% of the installed base in 2015

If TETRA was historically not available in the U.S because of the technology not being approved by the FCC until 2012, the technology is since then progressing. It is forecasted by IHS that the TETRA terminal market is set to grow by 14% by 2019, a large portion of the market being still using analog technologies.

By 2011, TETRA had been deployed in more than 130 countries, and more than half were located outside of Europe, most notably in Asia Pacific and Africa as the fastest developing regions.

4.5 Norms and regulatory context

If TETRA is an ETSI standard from the beginning, TETRAPOL, being an older technology but also much more mature at the beginning of TETRA in 1995, is also since 1996 recognized by the vast majority of the European and International bodies such as the ITU, CEPT, European Police Co-operation Council, ETSI Board and The Radio Communication Agency.

DMR is also an ETSI standard.

4.6 Level of security and threats

Being designed for use for private networks as well as for market where critical communication is a required feature, the level of security of digital technologies such as DMR, TETRA and TETRAPOL is considered as high. As an illustration, TETRA technology features following security capabilities:

- Encryption
- Authentication
- Key management

Despite the high level of security, some issues have been found in the past. A vulnerability was notably found in the authentication process of TETRA, with no data integrity protection mechanism, leading to the possibility for a false base station to intercept the initial authentication message.

In terms of environment, ATEX devices are available for TETRAPOL, TETRA and DMR technologies. The support of this certification is currently a driver for adoption in industries such as in the oil and gas sectors.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

4.7 Main equipment manufacturers

Manufacturers for each of the considered technologies are presented in the table below:

Table 17: PMR manufacturers

Technology	Manufacturers
TETRAPOL	EADS (Connexity) and Siemens (S-PRO)
TETRA	Motorola, EADS, Sepura, Teltronic, Rohill, Selex Communications, Rohde & Schwarz, Artevea, Damm, Sungar
DMR	Aselsan, Harris, Hytera, Kirisun, Radio Activity srl, Radio Data, Simoco, Tait communication , Yaesu

4.8 Capital and operating expenditure

It is estimated that around 23,400 TETRA base stations are deployed in Europe serving around 1.5 million users in Europe, ranging from governmental organization, public safety to utilities. TETRA and TETRAPOL users' needs are quite different from the needs of GSM-R users even though they may have similar requirement.

As noted previously in this report, the coverage requirements are quite different since complete portions of territory have to be covered (sometimes whole territory), including indoor, which makes a huge difference in terms of coverage requirement. TETRA and TETRAPOL use low frequencies in the 400 MHz range.

In terms of usage, the resilience of the network is very important for voice. Group Call, Push To Talk and Direct Mode Operations are very important for those users. One difference though with GSM-R is the fact that Direct Mode Operation is not a requirement for them and is not used on the ground.

In terms of backhaul, microwave is often used.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 18: Indicative cost elements for TETRA/TETRAPOL networks

EUR '000	TETRA/Tetrapol
CAPEX	
per TETRA/TETRAPOL sites	1400
per handset	900
per cab radio (in car)	2000
OPEX (% of CAPEX)each year	9%
Coverage (%pop/geographical)	
number of sites in EU+Norway	23450
number of TETRA/TERAPOL users ('000)	1500
number of user per site	64
Availability	

Source: European commission (SCF)

Table 19: Presentation of selected TETRA networks in Europe

Public safety TETRA networks	Number of users	sites	cost (EUR bln)	Cost per site (K EUR)
Austria	80 000	1800	1.1	611
Belgium	10 000	600	0.4	667
Denmark	20 000	500	0.2	400
Finland	30 000	1400	0.3	214
Germany	500000	4500	1.1	244
Italy	200000	3100	3.5	1129
Netherlands	85 000	600	0.5	833
Norway	40 000	2000	0.9	450
Sweden	50 000	1800	0.4	222
UK	300000	3500	5.5	1571

Source: Analysys Mason

4.9 Which evolutions in the next five years

DMR, TETRAPOL and TETRA have all been originally designed as voice and narrowband communication technologies. If for example TETRA saw a second release of its standard bringing improved throughputs up to 400 Kbps by using wider 150 KHz channels, it is commonly considered that those technologies will be, in a distant future, replaced by LTE or 5G to bring broadband applications to private networks.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

As earlier mentioned, several critical communication features specific to those technologies have already been standardized in latest 3GPP LTE Releases and the TCCA itself is cooperating within 3GPP for the further development of those features.

It is however difficult to tell when first LTE network supporting critical communication will be launched. Some countries are willing to do something quite rapidly. The U.S.A and South Korea for instance are working in this direction with their public safety network but the task has proven lengthy. In many situation, hybrid network will be launched to smooth a transition process that may well take several years.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

5 Short-range technologies

5.1 Synthesis

Table 20: Short-range technologies - synthesis

Short range technologies	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	+++ Already used in the industry, these technologies will likely continue to be used given their optimised consumption and are well suited for short range communications
Description	Short range technologies aimed at connecting devices, mostly in consumer places rather than in industrial environment
Standards and regulatory constraints	IEEE mostly and proprietary technologies
Area of operation	Worldwide
Protocols used	See detailed descriptions below
Security	-/+
Performances	High data rates over short distances
Range	Varies depending on the technology. A 433 MHz RFID tag can range up to 500m Bluetooth: 10m. BT smart up to 50m, BT 5.0 goes up to 200m Zigbee: 20/100m
Electrical consumption	Low power Battery lifetime - Bluetooth : months – Zigbee: years
Environmental aspects (ATEX, gas, temperature, CEM…)	Several implementations of equipment comply with ATEX directive,
Use sectors (public networks, industrial networks, future use for FoF)	Home networks, industrial networks
Maturity (TRL)	TRL9
Availability & associated constraints	Most technologies are widely available
Main providers	Siliconlabs, Qorvo, Atmel, Digi International, Freescale, Greenpeak, NXP, Renesas, Silicon Laboratories, STMicroelectronics, TI
Price of equipment	Chipsets and devices: a few €

Source: IDATE

5.2 Introduction

Many short-range technologies exist today and can be used in smartphones or dedicated devices. In this section, we describe the following technologies:

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

- Bluetooth
- Zigbee
- Z-Wave
- RFID/NFC
- Home RF
- UWB

The table below highlights the pros and cons of the short range technologies presented in this section

Table 21: Pros and cons of short-range technologies

	Pros	Cons
Zigbee	Standard Easy deployment (DIY) Ecosystem References Zigbee Green Power option	Battery lifetime Short range Lack of mobility management
Z-wave	Interoperable with 1700 products Ecosystem Indoor penetration	Proprietary
BLTE	Standard Ecosystem Easy to deploy	No backwards with Classic Bluetooth Not adapted for applications requiring continuous data transfer
UWB	High and variable throughput Adapted to geolocation and video streaming	Very limited range Mobility

Source: IDATE

The features of short-range technologies are presented in the table below:

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 22: Features of main short-range technologies

Features	Zigbee	Bluetooth	Wifi	Z-wave	UWB
IEEE	802.15.4	802.15.1	802.11a/b/g/n/	Proprietary technology	IEEE 802.15.3a
Storage requirements	4-32 KB	250 KB +	1 MB +	n/a	n/a
Battery lifetime (consumption)	Years	Months	Hours	Months	Months
Data rate transfer	250 Kbps	1 Mbps	11-54-108-320 Mbps	100 kbps	~100 Mbps
Range	100 m	10 m	300 m	100m	10 m

Source: IDATE DigiWorld, in *World M2M markets*, November 2016

5.3 Performances of short-range technologies

5.3.1 Bluetooth (802.15.1)

Bluetooth is a specification for the use of low-power radio communications to wirelessly link phones, computers and other network devices over short distances. The technology is ratified as IEEE Standard 802.15.1-2002. Wireless signals transmitted with Bluetooth cover short distances (power class dependent: from 1 to 100 metres, 10-20 indoor). Bluetooth devices generally communicate at less than 1 Mbps. The devices use a radio communications system, so they do not have to be in line-of-sight of each other. Devices communicate using protocols that are part of the Bluetooth specification. The major companies promoting the technology are Ericsson, Intel, Lenovo, Microsoft, Nokia, Motorola and Toshiba.

As a new standard, Bluetooth Low Energy marketed under Bluetooth Smart provides reduced power consumption (factor of 100 compared to Classic Bluetooth) mainly thanks to a packet format downsize (from 31 to 21 bytes) and at lower cost. The latest version, Bluetooth 5 operates at the same frequency as the Classic Bluetooth at 2.4 GHz, provides higher range (200m outdoor and 40m indoor), shortens latency and doubles the data rates (up to 2 Mbps). However, even though it meets multiple smart home expectations in terms of costs and consumption, it does not provide any advantage in the case of continuous data transfer. Additionally, the low power version is not backward compatible with the previous 'Classic' Bluetooth protocol, which is a major drawback in the case of a huge installed base.

Table 23: Bluetooth classes

Class	Maximum Power	Range
1	100 mW (20 dBm)	~100 m
2	2,5 mW (4 dBm)	~10 m
3	1 mW (0 dBm)	~1 m

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Source: ITU

In 2017, Bluetooth 5 was released bringing increased security, improved throughput up to 2 Mbps as well as up to 200m range. At this range, maximum throughput is however brought back to 1 Mbps

5.3.2 Zigbee (802.15.4)

Conceived in 1998, Zigbee is a specification designed for communication protocols using small and low power digital radios based on the IEEE 802.15.4 defined for the WPAN (Wireless Personal Area Network), standardized in 2003. The standard benefits from Zigbee Alliance created in 2002 which is a group of over 400 global companies that promote the standard.

Zigbee operates in ISM bands 868 MHz in Europe, 915 MHz in the US and Australia and 2,4 GHz in most countries around the world. It has been designed for applications requiring short range, low bitrate, long battery life, and a secure architecture. Actually, its bitrates supported vary from 20 to 250 kbps depending on operating frequency for at least a 2-year autonomous. The technology that supports a mesh network capability provides transmission distances from 10 to 100 meters line of sight indoor and up to 1500m outdoor.

Typical applications include smart meters. As a major commercial reference, Zigbee has been imposed as a technology of choice by the Department of Energy & Climate Change for electricity and gas smart meters in the UK. Basically, Zigbee can be used in multiple use cases but the open standard has especially been retained for home entertainment, and home and building automation providing unique language for a whole ecosystem including home monitoring, energy management, HVAC, security and comfort devices. Today, telcos and cablecos are among the major users of Zigbee which has been integrated in set top boxes, gateways or satellite transceivers. Names include Comcast, Time Warner Cable, EchoStar, DirecTV, Charter, Rogers, Deutsche Telekom, Videocon.

In addition, for its latest version, Zigbee has developed a new optional feature called Green Power that will be available for 2017. Zigbee Green Power allows the use of battery-less devices such as switches, sensors, dimmers that are not connected to the electricity grid. The devices are powered by using the environment like motion, light, vibrations…

Figure 10: Zigbee Alliance members involved in smart home

Source : Zigbee

5.3.3 Z-Wave

Z-Wave is a proprietary technology developed by Danish startup Zen-Sys and acquired by Sigma Designs in 2008. The technology operates in the ISM bands: 868.42 MHz in Europe, 908.42 MHz in the US and Canada and other frequencies in other countries depending on their regulations.

Z-Wave has been designed for low latency transmission of small data packets transferred at 100 kbps. Being optimized in a mesh architecture topology, the technology has an effective range at 100m thanks to the ability to hop the signals up to four times between nodes. Given the range and its indoor penetration capabilities to travel through thick walls, floors and ceilings, Z-Wave is convenient for home automation applications oriented to residential homes (control lighting, security, HVAC, home cinema, garage controls, etc…).

Actually, Z-Wave technology counts over 1700 certified interoperable products designed by brands making up the Z-Wave Alliance, an association of 450 companies. The alliance has been created to promote and expand the technology and especially focuses on interoperability of devices. Principal members of the alliance are major companies in the smart home and in security including ADT Corporation, FAKRO, Ingersoll Rand, Nortek Security & Control and Samsung (for SmartThings).

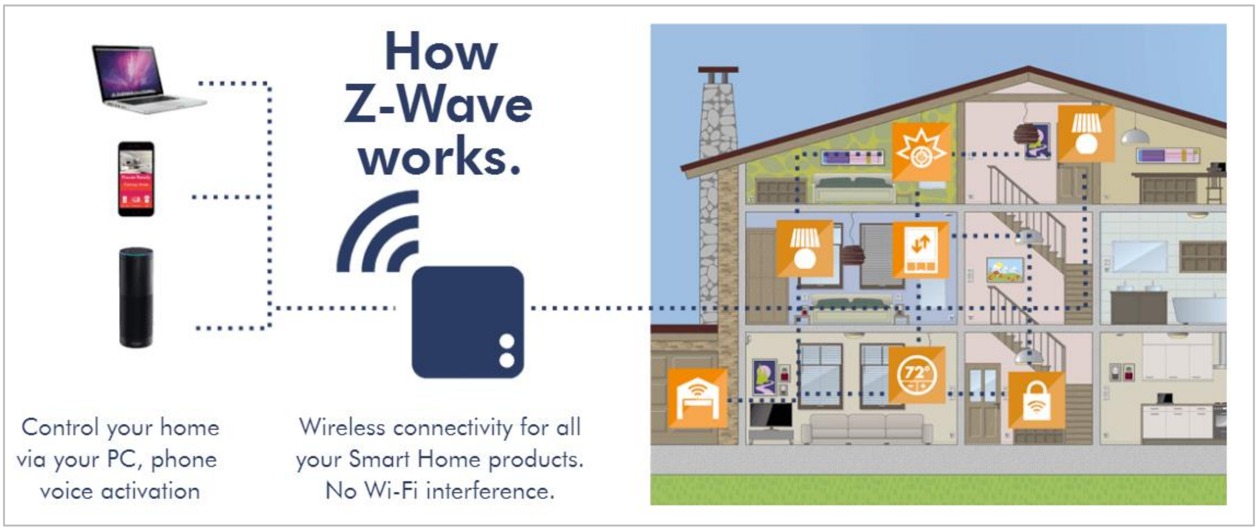
Z-Wave claims to be easy to install and a secure technology with multiple features involving AES encryption and device authentication.

Sigma Designs has also developed several versions of the protocols first in 2013 with Z-Wave Plus improving network improvements such as increasing the range at 150m, reducing the energy consumption by 2/3 and delivering 250% more bandwidth. Another version enhancing security features has been released in 2016 targeting the use of Z-Wave in security industry. Also as open source version has been developed.

As of 2016, over 50 million Z-Wave products have been launched. It is a technology of choice for most smart home products as illustrated by Orange Homelive based on Z-Wave.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 11: Z-Wave principle



Source: Z-Wave

Figure 12: Current protocols used per category of smart home devices

Product Category	Sample Size (# Products Purchasable in the U S)	Number 1 Radio Protocol		Number 2 Radio Protocol		Number 3 Radio Protocol	
Gateway / Hub	29	Wi-Fi	24%	Z-Wave	23%	ZigBee	17%
Plug	41	Z-Wave	43%	Wi-Fi	36%	Bluetooth	5%
Sensor: Door	26	Z-Wave	41%	ZigBee	24%	Wi-Fi	3%
Thermostat	23	Wi-Fi	58%	Z-Wave	21%	ZigBee	17%
Door Lock	19	Z-Wave	62%	Bluetooth	29%	Wi-Fi	5%
Light Bulb: Color	19	Bluetooth	42%	ZigBee	37%	Wi-Fi	11%
Scale	13	Bluetooth	67%	Wi-Fi	33%	N/A	
Light Switch	12	Wi-Fi	36%	Z-Wave	36%	Bluetooth	14%
Smoke Detector	9	Wi-Fi	33%	Z-Wave	22%	433 MHz	22%

Source: SmartHomeDB

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

5.3.4 RFID/ NFC

The NFC technology is a short range technology enabling the exchange of data between two devices. It basically allows applications such as mobile payment, mobile ticketing or smart poster providing further information on your device. It is also used to facilitate the pairing of two Bluetooth devices (for instance a smartphone and an audio device) and sometimes to provide location as well.

Technologically speaking NFC operates in the 13.56 MHz unlicensed frequency with a 2Mhz bandwidth allowing a data rates of up to 424 kbits. It is actually an extension of the iso 14443 standard for contactless identification card. Here are some advantages of the technology compared to other short range technology

- Very low power consumption (up to 1000 days). NFC technology may even work in situation where a device is not powered
- Its operating range of 10 to 20 cm allows a better security in the exchange of information in crowded areas which is especially important for financial transaction.
- This short operating range can be considered as less intrusive than Bluetooth since the user has to voluntarily carry its nfc enabled device in the area of the communicating object to initiate a communication
- Compatible with RFID
- Functions in 3 different modes. It can either provide information and behave like a contactless card as it is the case with RFID, either ask for information or communicate in both ways with another device
- Easy configuration and setup time. It can also be used to easily pair Bluetooth devices together whose long discovery time is a true drawback

Initially well deployed in Japan and in other Asian countries, it can now be found in multiple places most notably in the transportation and at the point of sales. For this last use case, it is to be noted that NFC is more used through credit cards embedding NFC technology rather than in smartphone where usage is still limited. This last fact is however changing with Apple and Google solution Apple Pay and Google pay which are gradually deployed in countries all over the world

5.3.5 Home RF

Home RF (Home r*adio* f*requency) was d*esigned specifically for wireless networks in homes - in contrast to 802.11, which was created for use in businesses. HomeRF networks were designed to be more affordable to home users than other wireless technologies. Based on frequency hopping and using the 2.4 GHz band for the transmission of voice and data, HomeRF has a range of up to 150 feet. HomeRF uses Shared Wireless Access Protocol.

Home RF was developed in 1998 by the Home Radio Frequency Working Group, a consortium of mobile wireless companies that included Proxim Wireless, Intel, Siemens AG, Motorola, Philips and more than 100 other companies. The Home Radio Frequency Working Group was disbanded in January 2003 after other wireless networks became accessible to home users. As a result, HomeRF fell into obsolescence.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

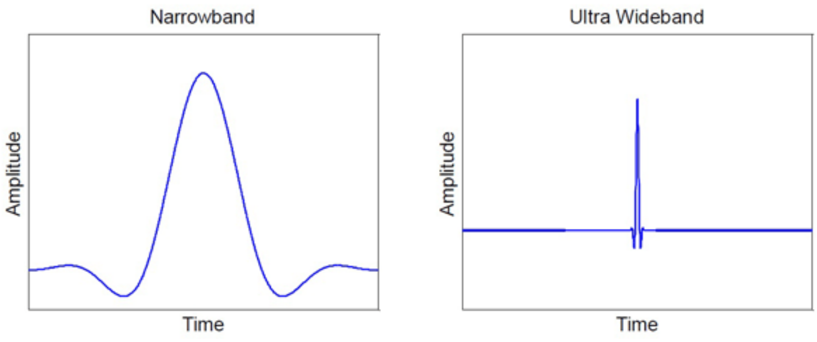
5.3.6 UWB

UWB or Ultra Wide Band ratified under the IEEE 802.15.3a has been designed for use in Personal Area Network but the task group was dissolved in 2006. Today, UWB is more seen as a method of radio transmission - and not a standard - that offers a broad variety of use cases.

The technology which operates in unlicensed frequency bands from 3.1 to 10.6 GHz has the particularity to send short signal pulse over a wide band of RF (500 MHz) at ultra power level. UWB works at short range level with optimum data speeds of 480 Mbps at 2-3 meters that drop to 100 Mbps at 10 meters but according to the specifications the technology can provide up to 2 Gbps. As a consequence, UWB has a wide area of applications from video streaming between entertainment systems within a house to sensor data or security camera streams. A key application for UWB is the Wireless USB to replace the traditional USB cable. Also, the latest interest from the industry for UWB is the ability to provide higher accuracy for location and imaging devices (location tracking applications, precision location within buildings). Typically, UWB characteristic is to measure distance and location with the accuracy of 5 to 10 cm compared to meters in the case of narrowband technologies.

Today, UWB is governed by the WiMedia Alliance composed of over 350 members who are in charge of defining, certifying and supporting wireless technology for multimedia applications. Members include names as Samsung, Dell and Toshiba.

Figure 13: Difference with narrowband and Ultra wideband signal



Source: Electronic Design

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

6 WiFi

6.1 Synthesis

Table 24: WiFi technology - synthesis

WiFi	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	+ Will continue to be used in the industry and could integrate latest evolutions (mesh networking, use of 60 GHz band) in order to increase performances. Competition is likely in the unlicensed 5 GHz band from 4G in MulteFire mode. More integration with 5G is to be expected from 2020 on.
Description	Wireless Local Area Network application (with focus on broadband application)
Standards and regulatory constraints	IEEE
Area of operation	Worldwide
Protocols used	OFDMA
Security	+ 802.11i or WPA2 provides a better security than WEP
Performances	Provide very high data rates over short distances
Range	Up to 200/300 m
Electrical consumption	Around 25w for enterprise grade access points in 802.11ac Battery lifetime: hours
Environmental aspects (ATEX, gas, temperature, CEM…)	Several implementations of equipment comply with ATEX directive
Use sectors (public networks, industrial networks, future use for FoF)	Public network, industrial networks, future use for FoF
Maturity (TRL)	TRL 9 for 802.11a, b, g, n, ac, ad, ah TRL 8 for 802.11.ax TRL 6 for 802.11.ay
Availability & associated constraints	Wide availability
Main providers	HP (previous acquisition of Aruba Networks), Cisco, Aerohive Networks, Ruckus Wireless, Zebra
Price of equipment	Router: €50 to 200

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

6.2 Performance of WiFi systems

WiFi, as standardised by IEEE, uses unlicensed frequency bands in the 2.4 and 5 GHz frequency bands but with the time support for other frequency bands such as the 60 GHz and 900 MHz band has been added to support new use cases. The latest technical improvements involve wider bandwidth and the use of MIMO to boost data rates. The various WiFi generations and their respective characteristics are presented in the table below.

Table 25: WiFi generations

WiFi generation	Launch date	Frequency band	bandwidth	Theoretical peak throughput	MIMO	Outdoor range
802.11a	1999	5 GHz	20 MHz	54 Mbit/s	No Support	~110 m (5 GHz)
802.11b	1999	2.4 GHz	22 MHz	11 Mbit/s	No Support	~130 m
802.11g	2003	2.4 GHz	22 MHz	54 Mbit/s	No Support	~130 m
802.11n	2009	2.4 et 5 GHz	20 MHz, 40 MHz	Up to 600 Mbit/s (4x4 MIMO and 40 MHz bandwidth)	Up to 4 x 4	~240 m
802.11ac	2012	5 GHz	20, 40, 80 ou 160 MHz	Up to 6.77 Gbit/s (8 x 8 MIMO and 160 MHz bandwidth)	Up to 8x 8	n/a
802.11ad	2013	60 GHz	2160 MHz	Up to 7 Gbps using beamforming		n/a
802.11af	2013	470-710 MHz (TV White Spaces)	Up to 8 MHz	Up to 568 Mbps with 4x4 MIMO (35.6 for 8 MHz)	Up to 4x4	Up to more than 1 km
802.11ah	2016	< 1 GHz (depends on regions)	1,2,4,8,16 MHz (depending on frequency bands)	Up to 8 Mbps		Up to 1 km
802.11ax	2018-2019	2.4 & 5 GHz	Up to 160 MHz	4x increased average throughput in dense areas , up to 10 Gbps (peak)	Up to 8x8 (5 GHz) and 4x4 (2.4 GHz)	
802.11ay	2019	60 GHz	Up to 8640 MHz	Up to 20-30 Gbps		10m

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

802.11ac is now being implemented in a variety of devices including smartphones and tablets. The 60 GHz band will be used by the 802.11ad version of WiFi and will allow very high data rates for short-range communications. It is already available in a limited number of commercial devices.

6.2.1 802.11a and 802.11b

WiFi generations 802.11a and 802.11b were developed at the same time and the two generations were released at the same time in 1999.

802.11a delivers a theoretical data rate up to 54 Mbit/s in the 5 GHz band. The use of higher frequencies leads to an increased sensitivity to obstacles. Besides the higher cost of implementing 802.11a, WiFi led the 802.11b generation to quickly become more popular than the 802.11a standard. Furthermore, due to the difference in implementation cost, the 802.11a standard found itself being used principally by businesses while 802.11b spread widely among consumer products, to such a point that many users think that 802.11a was developed after 802.11b.

The 802.11a and 802.11b standards are incompatible with each other. Even if some vendors have marketed multi-mode networks working with both WiFi generations, such cases have been very few and far between, and such networks were not common.

6.2.2 802.11g

Products supporting the 802.11g WiFi generation emerged on the market in 2003. The purpose behind the new standard was to adopt the positive aspects of both 802.11a and 802.11b. It means a high data rate working in the 2.4 GHz band. This detail allowed 802.11g devices a full compatibility with 802.11b networks and vice-versa.

Due to widespread popularity, the already-crowded 2.4 GHz band had to support large numbers of mobile devices especially laptops that were converted from dual-mode (a/b) to tri-mode (a/b/g). This led to a certain degree of nuisance from interference, especially with Bluetooth equipment.

6.2.3 802.11n

Released in 2009, the WiFi 802.11n generation experienced the strongest and fastest rate of adoption ever known among WiFi standards. This new standard was developed to improve the data rate supported by the 11g standard through using MIMO.

Since there was undoubtedly a significant gain in performance between 802.11g and 802.11n standards, the rates of migration from 11g and the adoption of 11n by businesses were unprecedented. Indeed, one-third of businesses indicated, sometime before the 802.11n release, that they were ready to migrate to or adopt 802.11n by the end of 2010.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Besides, high download rate capacities made the 11n generation the ideal candidate for multimedia usage. In less than three years between 2009 and 2012, this generation was implemented on almost all currently commercialised mobile devices, ranging from smartphones to laptops including tablets.

By December 2012, the transition to 802.11n was almost complete with 84% of WiFi access point shipments based on the WiFi 802.11n generation.

6.2.4 802.11ac

Released in December 2012, the 802.11ac generation allows functioning with several configurations depending on the choice of bandwidth (from 20 MHz to 160 MHz) and the MIMO setting (up to 8×8).

Given that every configuration allows a certain data rate, scenarios of use present the possibility of adopting the configuration by the type of device on which 802.11ac is implemented. For example, television sets with 4K resolution can be configured up to 8×8 MIMO using a bandwidth of 160 MHz for ultra-HD streaming. Meanwhile, handheld devices can function with a single antenna configuration on 80 MHz bandwidth.

This flexibility will certainly be one of the major elements in the widespread dissemination of the 802.11ac generation.

During the MWC 2013 in Barcelona, the South Korean operator SK Telecom demonstrated WiFi routers working on 802.11ac and able to deliver data rates up to 1.3 Gbit/s. The carrier indicated its intent to bring these routers to market during 2013. As for the implementation of the standard in access points and mobile devices, the first products were expected to be shipped in Q3 2013, thereby boosting the growth of the WLAN market. It passed the milestone of 1 billion USD for the first time at the end of 2012.

802.11ac chips have started shipping in significant quantities in 2013. It was expected that, by the end of 2014, 802.11ac would be included in close to 50 per cent of all WiFi systems produced. While not initially devised as a technology for mobile devices, it has been progressively adopted by handset manufacturers for their high-end devices. According to the Wireless Broadband Alliance, in 2014, 2/3 of IEEE 802.11ac products were smartphone devices. These devices, however, only offer a single stream solution, meaning they do not support MIMO, nor the full speeds enabled by the technology.

6.2.5 802.11ad or WiGig

IEEE 802.11ad is operating on the unlicenced 60 GHz band and offering throughputs in the range of 4 to 8 Gbps over very short distances and does not penetrate walls. It is not compatible with 802.11ac and will have to be supported

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

alongside. Because of the limited range, 802.11ad, also called WiGig, will be used in different situation, especially in the digital home for fast content exchange, video mirroring on the television and so on.

As soon as 2015, devices supported this technology alongside the other flavours of WiFi. The Snapdragon 810 chipset from Qualcomm is already supporting 802.11ad.

At the end of 2017, it appears that 802.11ad has not yet created its ecosystem and Intel is likely to drop support to this technology. Qualcomm still supports 802.11ad and announced recently that ASUS will integrate it into a smartphone. Use of WiGig for backhaul of 5G base stations is seen by some players as an interesting move.

6.2.6 IEEE 802.11 at the era of 5G

While 4G Radio Access Technology is set to evolve toward 5G around 2020, WiFi too is set to continue to evolve toward a technology that support new business models and new use cases.

In the recent years, WiFi has evolved toward carrier-grade capability and although adoption and deployment still has to move to mass deployment, the technology is now capable of managing subscriptions, handling QoS, sustaining Gbps throughputs while allocating resources to specific users or type of communication, all this while being more integrated in network operators, whether cable or cellular.

These technologies, among others, are HS2.0, community hotspot, WiFi calling, 802.11ac with MU-MIMO, and 256-QAM modulation.

In the future, IEEE 802.11 technology is set to adapt to new challenges in order to address needs that are not currently addressed by WiFi. Fields identified by WBA are:

- Enterprise communication and public safety
- Integration with other networks: the ability to discover other service around through WiFi aware in order to enable proximity-based marketing and services. WiFi aware brings a beacon behaviour to WiFi. WiFi is then able to broadcast small messages.
- Machine Type Communication (smart city, smart healthcare…): 802.11ah and 802.11ax for high density areas
- TV everywhere

The key here to address those needs will be the integration capability of WiFi with other technologies and to new environment. Collaboration is seen as strength of 802.11 technologies and complementarity with Wireless Personal Area Network (WPAN) technologies such as Bluetooth, Zigbee, ANT+ or with Low Power Wide Areas (LPWA) technologies for smart city such as SIGFOX or LoRA will be critical.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

WiFi also needs to adapt, Work has already be achieved with WiFi Aware for easier service discovery. Improvements include:

- Operation in new frequency bands ((802.11ad for the 60 GHz band, 802.11ah for the band below 1 GHz or 802.11af)
- WiFi is able to operate on new bands
- WiFi works in the TV White Spaces or, last but not least, with 802.11ax to work in high density scenario. WiFi will also have to be capable of being fully integrated in network OSS/BSS and SON features will have to be developed to take into account the existence of WiFi as an element of the network.

6.2.6.1 802.11ah

IEEE 802.11ah is an adaptation of WiFi to work on sub GHz frequency bands. The appeal of this variant of WiFi is mainly its extended range compared to 2.4 GHz and 5 GHz and the resulting reduction in energy consumption. As a result, 802.11ah will target internet of things application, enabling the creation of large groups of sensors. The standard was expected to be finalised in 2016 but first chips could enter the market in 2015. As a result from its specification, 802.11ah is not a technology aimed at being used for carrier WiFi or as an offload technology.

ISM ALLOCATIONS APPLICABLE FOR IEEE 802.11AH	
COUNTRY	BAND LIMITS (MHZ)
China	755 - 787
Europe	863 - 868
Japan	916.5 - 927.5
Korea	917.5 - 923.5
Singapore	866 - 869 & 920 - 925
USA	902 - 928

Source: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11ah-sub-ghz-wifi.php

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

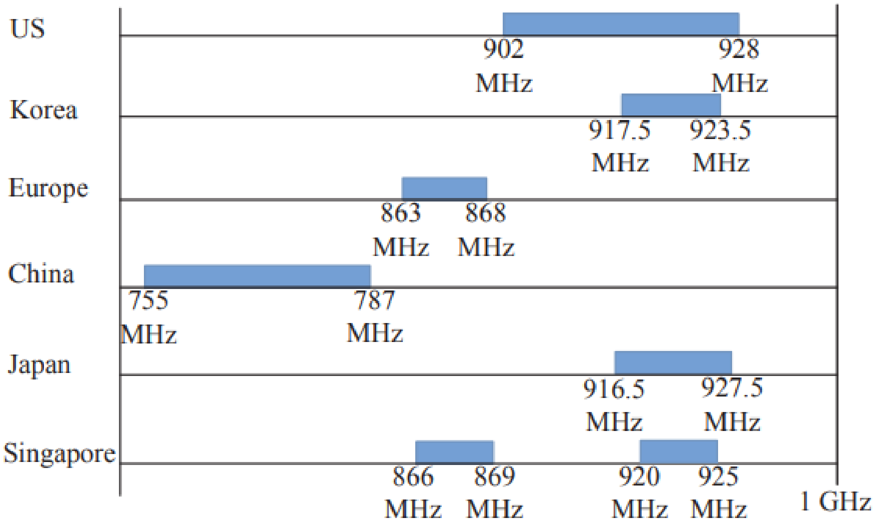


Figure 3 Sub 1 GHz spectra specified in the 802.11ah channelization.

Source: https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_115.pdf

6.2.6.2 802.11ax

IEEE 802.11ax is still in an early stage of development. It should be seen as the successor of 802.11ac when 802.11ay will be the successor of 802.11ad, which is operating on the 60 GHz unlicensed band. Contrary to 802.11ac, it will work on both 2.4 and 5 GHz frequency band. It will marginally increase peak throughput to up to 10 Gbps but more importantly, this version of the standard will significantly improve average throughputs in very crowded environment and in difficult areas to reach.

It has been found, for instance, that a typical throughput that could be reached at the edge of an 802.11ac network could be improved by 20 to 30%.

In order to reach this level of performance 802.11ax will notably leverage technologies such as OFDMA, MU-MIMO and 1024 QAM.

First 802.11ax products will be launched in 2018. First chipset supporting 802.11ax have been sampled but it should take more time for end-user products to embed those chipset.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

6.2.6.3 802.11ay

802.11ay is to be understood as an update to 802.11ad standard operating on the 60 GHz. While 802.11ad used a bandwidth of 2160 MHz, the .ay version will use even larger 8640 MHz bandwidth to bring maximum throughputs in the range of 20 to 40 Gbps per stream. With 4x4 MIMO configuration, the maximum and theoretical speed could reach 176 Gbps.

The draft 1.0 of the standard is expected to be published in November 2017, which means that pre 802.11ay products could be released by the end of 2018 and products complying with the final standard could arrive one year later in 2019.

6.2.7 WiFi in industrial environment

Industrial Wireless LAN differs from the Wireless LAN (WiFi) at home as it generally involves radio Planning with dedicated tools (plus channel redundancy and cell redundancy with overlapping) and provides deterministic WLAN capabilities. The latter is provided with:

- band reservation (TDMA coexists with CSMA/CA);
- PCF and iPCF: each client has a 2 ms timeslot assigned.

For any new installation using the 802.11 “family”, IEEE 802.11n seems to be the WiFi standard of choice. 802.11n increases data throughput compared to IEEE 802.11 b or g, although this is often not the prime concern. It also uses spatial information, which means that waves reflected from walls or steel structures are used just as direct waves are for retrieving the data. Therefore, IEEE 802.11n offers much better stability of the data streams especially in industrial environments where a lot of large structures and metal objects are common.

Wireless Profitbus is also part of the Industrial WLAN systems. For information on Wireless Profitbus, please refer to section 8.2.4.

6.3 Geographical market

While an IEEE technology, WiFi can be found all over the world. First integrated into laptop, WiFi has then be embedded in smartphones and a very large range of products, from balance to smartwatches, going through tablets and Smarthome products.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

6.4 Norms and regulatory context

WiFi technologies are standardized within the Institute of Electrical and Electronics Engineers (IEEE). WiFi technology is leveraging unlicensed frequency bands and as such is subject to some regulations related to the use of unlicensed spectrum, such as the use of Listen Before Talk mechanism that prevent to interfere with other users.

In terms of support for specific environment, ATEX compliant equipment is available on the market with support for up to Zone 1 for gas and Vapor and 21 for dust. Both ATEX compliant and hardened enclosure are available and access point designed from the outset to comply with ATEX environments. Zone 0 and 20 hardware do not seem to be available.

6.5 Level of security and threats

Security of WiFi standard has evolved a lot throughout the year, with encryption mechanism seen as the best way to protect the network. WEP was first used but shortly hacked. This resulted in the development of WiFi Protected Access (WPA) which was also superseded by WPA because of security holes. WPA2, which has replaced WPA is available in two different modes:

- Personal (Pre Shared Key)
- Enterprise, where a RADIUS server is required

It is to be noted that a configuration mode called WPS (WiFi Protected Setup) is available where pushing a button on the box and the client ease the “pairing” process but a flaw in security leaves it vulnerable to brute force attack.

6.6 Main equipment manufacturers

Below is a list of the top 5 WiFi equipment vendors in 2015 by revenues:

- HP (previous acquisition of Aruba Networks)
- Cisco
- Aerohive Networks
- Ruckus Wireless
- Zebra

The two first vendors are generalist network equipment manufacturers with end to end solutions while the three following are WiFi specialists.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

6.7 Which evolutions in the next five years?

By 2022, WiFi technologies and 5G will continue to converge and be more and more integrated. While 3GPP technologies are investing the unlicensed spectrum, which is WiFi traditional foothold, there will likely still be a place for both group of technologies, WiFi performance continuing to make progress.

6.8 Maturity of the ecosystem in the years to come

IEEE 802.11 ecosystem will continue to be as mature as it is today in the years to come. 3GPP support for unlicensed frequency bands with LTE-U and LAA may however limit the WiFi market, especially if the standalone version of LAA called MuLTEfire is successful. However, given the current adoption of WiFi technology, it is not very likely to kill this ecosystem.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

7 WiMAX

7.1 Synthesis

Table 26: WiMAX technology - synthesis

WiMAX	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	- The WiMAX technology is being replaced by TD-LTE all around the World. There might be some use for industrial applications but the lack of support from the industry will soon lead to its end
Description	Wireless Local Area Network application (with focus on broadband application)
Standards and regulatory constraints	IEEE 802.16
Area of operation	Worldwide
Protocols used	OFDMA
Security	++
Performances	Provide very high data rates over short to medium-range distances
Range	A few km
Electrical consumption	1 day (smartphone)
Environmental aspects (ATEX, gas, temperature, CEM…)	Several implementations of equipment comply with ATEX directive?
Use sectors (public networks, industrial networks, future use for FoF)	Public network, industrial networks, future use for FoF
Maturity (TRL)	TRL 9
Availability & associated constraints	Fair availability
Main providers	Huawei, ZTE?, Nokia?
Price of equipment	Base station: ~€100K Devices: €~200-500

Source: IDATE

7.2 Performances of WiMAX technology

While WIMAX was originally considered as a disruptive technology, it did not manage to grab interest to the exception of some operators in the world. The technology was rather used as a fixed wireless broadband technology The lack of ecosystem resulted in costly equipment with often interoperability issues that didn't help the technology to take off.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 27: Mobile WiMAX characteristics

Mobile WiMAX	
Max throughput per sector (DL=downlink UL=uplink)	DL: 20 Mbps (14 MHz channels)
Bandwidth	1,5-14MHz
Frequency bands	2.3-2.5-3.5 GHz
Multiplex mode	sOFDMA
Duplex mode	TDD/
Standard	IEEE 802.16-2005

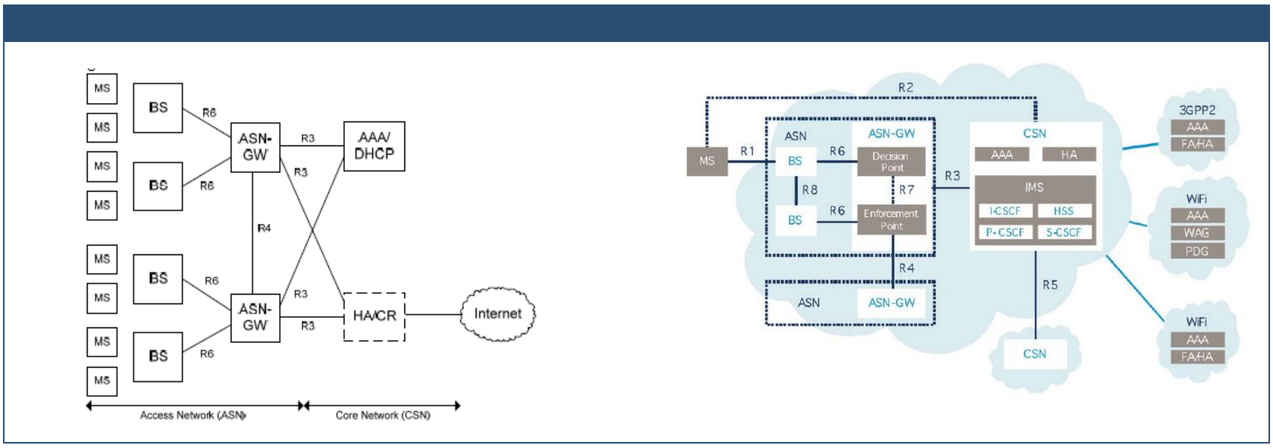
After the failure of the development of the Wireless Local Loop in the years 2000, WIMAX indeed appeared as a mature technology capable of supporting multiple Mbps without line of sight, something that was much looked for grey areas. Technologically in advance over other legacy 3GPP technologies WIMAX however suffered from a lack of industrial support and the hardware ecosystem failed to develop, to the extent that no WIMAX carrier in France eventually deployed the number of site that their license legally required.

In October 2007, WiMAX, developed by the WiMAX Forum as port of the IEEE was also recognized as being part of IMT-2000 technologies and thus 3G.

It is to be said nonetheless that WIMAX technology was deployed on large scale abroad for fixed as well as mobile usage. In Japan, KDDI was notably known for its WIMAX network deployed by its sister company UQ Communication reaching 4.1 million subscribers by the end of 2015. Since then the technology has evolved to become compatible in its WIMAX 2 version with TD-LTE, one flavor of 4^{th} Generation technology LTE.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 14: Mobile-WiMAX architecture



Source: WiMAX Forum

Mobile WiMAX date rates according to the antenna configuration are the following:

Table 28: Mobile-WiMAX data rates

DL/UL Ratio			1:0	3:1	2:1	3:2	1:1	0:1
User Peak Rate (Mbps)	SIMO (1x2)	DL	31.68	23.04	20.16	18.72	15.84	0
		UL	0	4.03	5.04	6.05	7.06	14.11
	MIMO (2x2)	DL	63.36	46.08	40.32	37.44	31.68	0
		UL	0	4.03	5.04	6.05	7.06	14.11
Sector Peak Rate (Mbps)	SIMO (1x2)	DL	31.68	23.04	20.16	18.72	15.84	0
		UL	0	4.03	5.04	6.05	7.06	14.11
	MIMO (2x2)	DL	63.36	46.08	40.32	37.44	31.68	0
		UL	0	8.06	10.08	12.10	14.12	28.22

Parameters: 10 MHz channel, 5 ms frame, PUSC sub-channel, 44 data OFDM symbols

Source : WiMAX Forum

Mobile WiMAX main characteristics are the following:

Parameters	Value
Number of 3-Sector Cells	19
Operating Frequency	2500 MHz
Duplex	TDD
Channel Bandwidth	10 MHz
BS-to-BS Distance	2.8 kilometers
Minimum Mobile-to-BS Distance	36 meters
Antenna Pattern	70° (-3 dB) with 20 dB front-to-back ratio
BS Height	32 meters
Mobile Terminal Height	1.5 meters
BS Antenna Gain	15 dBi
MS Antenna Gain	-1 dBi
BS Maximum Power Amplifier Power	43 dBm
Mobile Terminal Maximum PA Power	23 dBm
# of BS Tx/Rx Antenna	Tx: 2 or 4; Rx: 2 or 4
# of MS Tx/Rx Antenna	Tx: 1; Rx: 2
BS Noise Figure	4 dB
MS Noise Figure	7 dB

Table 7: Mobile WiMAX System Parameters

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

8 Short-range industrial technologies

8.1 Synthesis

Table 29: Short-range industrial technologies - synthesis

Short range industrial technologies	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	+ to ++ Many short-range industrial technologies answer to specific needs and environments. They will likely be used in the coming years as replacement cycles are quite long. Competition from 5G might come in the long term
Description	Short range technologies aimed at connecting sensors in the factory, mostly for monitoring, control, automation and analytics
Standards and regulatory constraints	IEC, IEEE
Area of operation	Worldwide
Protocols used	See detailed descriptions below (Frequency Hopping Spread Spectrum, TDMA)
Security	++
Performances	9.6 kbps to 4 Mbps
Range	Up to 250m in line of sight, can be extended with MESH capabilities (e.g. WHART)
Electrical consumption	<5W for a WHART gateway
Environmental aspects (ATEX, gas, temperature, CEM…)	Several implementations of equipment comply with ATEX directive,
Use sectors (public networks, industrial networks, future use for FoF)	Industrial networks
Maturity (TRL)	TRL9
Availability & associated constraints	Still a relatively fragmented market with a lot of competing technologies and not always interoperable between them
Main providers	ABB, Emerson, Endress+Hauser, Pepperl+Fuchs, Siemens, Schneider Electric, GE, Dust networks, Endress+Hauser, CDS
Price of equipment	N/A

Source: IDATE

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

8.2 Performance of short-range industrial systems

8.2.1 Wireless HART and ISA100a

8.2.1.1 Presentation

WirelessHART is a wireless communication technology used in industrial environment to monitor various flows, pressure, temperature and other wireless sensors. Based on IEEE 802.15.2-2006 radio protocol (Zigbee) and operating in the 2.4 GHz unlicensed frequency band, it is used for its low power and high speed capabilities as well as for its self-organizing and self-healing mesh network architecture. WHART is based on HART protocol, which is available since 1989 on the market as a wired and analog way of controlling sensors on the field. The rationale behind the development of this technology was to ease the deployment of HART on the field and also better leverage information stored on the device. From the beginning, the technology was devised as a multi-vendor interoperable solution.

The work on this technology started in the year 2004 with the contribution of 37 different companies of which ABB, Emerson, Endress+Hauser, Pepperl+Fucgs, Siemens, all part of the HART Communication Foundation which was funded with the purpose of developing this technology. The technology was launched on the market in September 2007 and at the same time the International Society of Automation (ISA) was offered a royalty free unrestricted access license. This lead to the development of a similar but nonetheless somewhat different technology called ISA100a. ISA100a is notably considered as bringing more flexible time scheduling as well as software tunneling and support for star and mesh topologies at the same time

Since 2010, Wireless HART it is also recognized as an International Electrotechnical Commission (IEC) standard as IEC 62591 and since 2014, it is also recognized as a Chinese national standrd

WART performances are presented in the table below:

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 30: WirelessHART characteristics

Attributes of *Wireless*HART

ITEM	DESCRIPTION
Based on Industrial Standards	HART- IEC 61158 *Wireless*HART - IEC/PAS 62591Ed.1 EDDL - IEC 61804-3 Radio & MAC - IEEE 802.15.4(TM)-2006 IEC/PA
Radio standard	IEEE 802.15.4-2006 @ 250kbps
Frequency Band	2.4GHz
Frequency Management	Channel hopping on a per packet basis
Distance	Up to 250m line-of-sight between devices
Power Options	Line Powered or Battery Powered
Topologies	Mesh, Star, Combined Star & Mesh

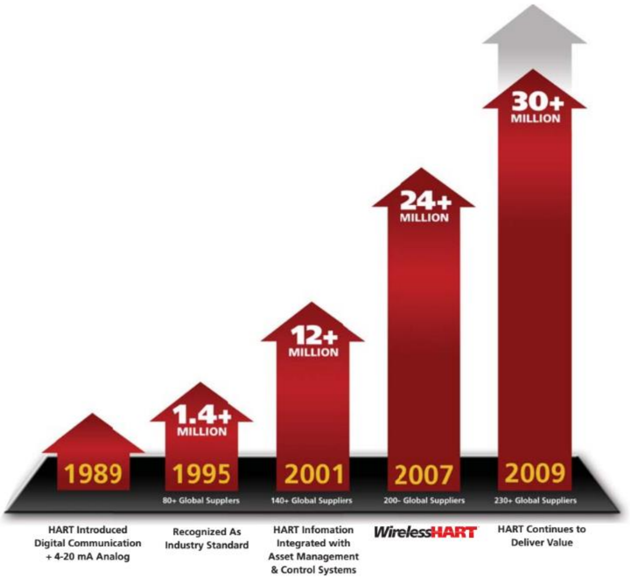
Source: Wireless HART

8.2.1.2 Adoption

While HART is widely adopted in the industry, with more than 30 million HART devices installed worldwide, WirelessHART still has potential for growth. As of mid-2012, about 39% of surveyed end users had adopted Wireless HART, up from 10% in 2010. As of 2017, it is considered that in the process automation market, Wireless HART is still dominant in terms of market share but that ISA100a is growing at a much faster rate.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 15: HART installed base



Source: Wireless HART

8.2.1.3 Limits

Both WirelessHART and ISA100a lack advanced cyber security features. Also despite their mechanism to limit interference, their functioning in the 2.4 GHz unlicensed band require some frequency planning, antenna location, and antenna separation, one reason why, despite its usefulness on the paper, integrating both WirelessHART or ISA100a with WiFi is difficult and not necessarily a good solution. All the more than WiFi is evolving at a much faster pace that command more frequent update that WHART or ISA100a.

8.2.2 WISA (WSAN)

While WHART was designed for process automation, WISA was designed for the factory automation.

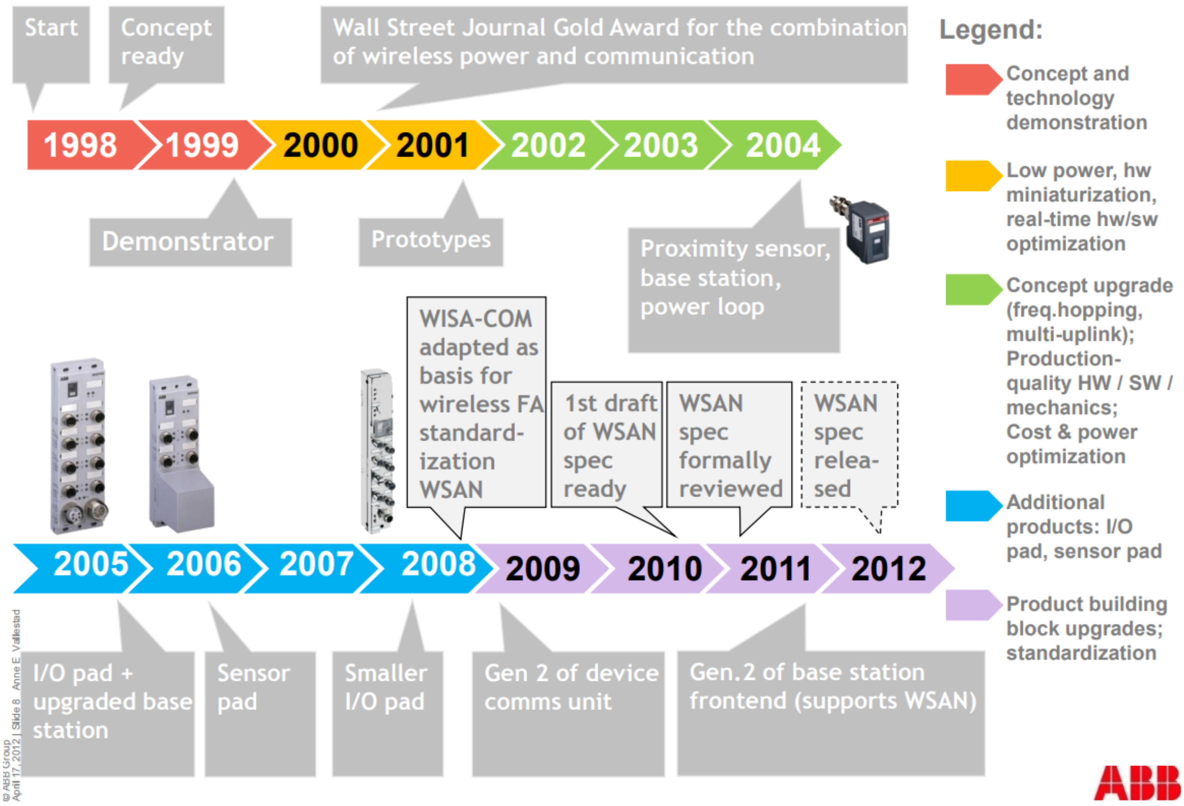
WISA, which stands for Wireless Interface to Sensors and Actuators is a technology developed by ABB in the years 2000. The idea was to release a technology that would solve both cost and performance issues in factory automation where up to 10,000 field devices can be used with very stringent reliability requirement. While those devices have

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

been wired for years, this has raised both deployment, cost and performance issues, something that WISA was developed to cope.

WISA operates in the unlicensed ISM 2.4 GHz band, the same band used by technologies such as Bluetooth, WiFi (802.11), Zigbee (802.15.4) and other technologies. It supports real time applications and its architecture is a typical star architecture similar to WISA-COM architecture is similar to cellular network with re-use of frequencies. Several base stations are thus deployed all over the factory to enable frequency reuse and each of those base stations are themselves connected to the control network through field bus technologies. In terms of protocols, it notably relies on TDMA, FDD and Frequency Hopping.

Figure 16: WISA-WSAN timeline (1998-2012)



Source: ABB

First devices based on this technology were released in 2003 with the first serial equipment being launched in 2004. In 2012, the communication part of the technology (WISA-COM) was given to standardization while the Wireless

Power part of the technology remained proprietary. Its name changed from WISA to WSAN (Wireless Sensor Actuator Network) and the technology is now being standardized by Profibus International.

Table 31: WISA versus Bluetooth

Requirement	WISA	Bluetooth*
Operating Frequency	2.4 GHz	2.4 GHz
Communication Bandwidth Raw bit rate	1 Mbps (DL) 4x1 Mbps (UL)	1 Mbps (DL/UL)
Communication Latency Nominal typical Worst-case (heavy disturbance -> retransmitts; max. No. of act. slaves)	2 ms < 5 ms 20 ms	5 ms 18 ms > 100ms
Node Density Number of active slaves per master Number of parked slaves per master	≤ 120 -	7 (256 **)
Power Consumption Active Sleep mode	200 mW 0.1 mW	300 mW 4 mW

* Infineon Flinkstone; ** 1-3s wake up time!

8.2.3 IEEE P1451.5

IEEE 1451.5 is a standard for smart transducer interface for sensors and actuators. It does not constitute a wireless technology.

8.2.4 Wireless Profibus

Profibus (Process Field Bus) is a standard that is used in automation technology and that was first promoted at the end of the 1980s by the German Department of education and research and then used by Siemens. Profibus is known as part of IEC 61158 standard. It can be used with several radio communication technologies such as Bluetooth, DECT, 802.11a, 802.15.4 ….

As of today, two main variants of Profibus protocols are used:

- Profibus-DB (Decentralized Peripherals) is used to connect active devices and detectors to a central controller.

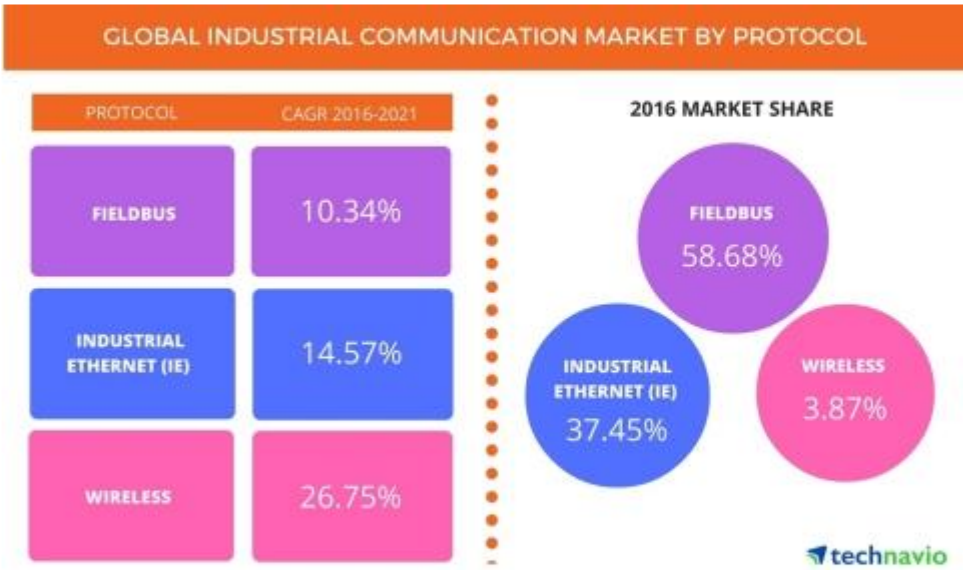
NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

- Profibus-PA (Process Automation) is used for monitoring and measurement equipment. It has been more specifically designed for hazardous environment (explosion notably)

Profibus is mostly used in Europe. As of 2009, more than 30 million Profibus nodes were installed, of which 5 million in industrial environment. However, because Ethernet protocol is largely deployed, other options are now preferred such as Profinet or Modbus/TCP.

As of 2015, industrial Ethernet accounted for 37% of the market.

Figure 17: industrial communication market in 2015



Source: Technavio

Wireless technologies used with Profibus must respect maximum throughputs depending on the distance to cover

Table 32: Maximum authorized distance depending on throughput

Throughput (kbps)	9,6	19,2	45,45	93,75	187,5	500	1 500	3 000	6 000	12 000
Distance (in m)	1 200	1 200	1 200	1 200	1 000	400	100	100	100	100

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

8.3 Geographical market

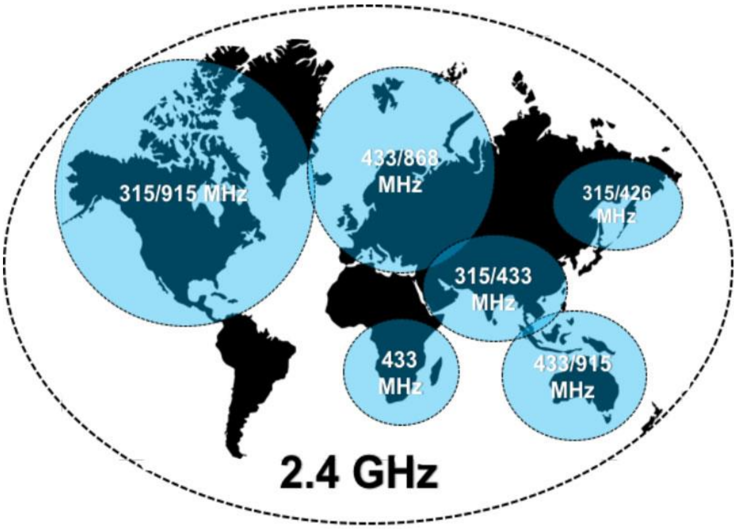
The market for wireless sensor communication technologies is the most developed in the United States and Asia with the biggest potential of growth because of the growing industrialization in the region.

It is to be noted here that the wireless industrial communication technologies market is still limited as wires are still predominantly used in the factories. It is estimated by IHD that in 2012, Wireless technologies accounted for only 2% of the total industrial communication market

8.4 Norms and regulatory context

Industrial communication technologies mostly operate in the ISM band and most specifically in the 2.4 GHz band. This can be explained because the 2.4 GHz band is the most common band around the world whereas other parts of the ISM band are specific to such or such region of the world

Figure 18: ISM band allocation in various regions of the world



Source: Ingenu

In terms of norms and standardization several organizations are involved depending on the technology considered. Industrial communication technology often started as proprietary technologies developed by companies in need for a specific solution before the standardization process really start and the standard is recognized by some sort of regional or international standardization body such as the International Electrotechnical Commission (IEC). WISA for instance is recognized as IEC 62591.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

8.5 Level of security and threats

Short-range industrial communication technologies have been designed to handle security properly, supporting more or less robust authentication and encryption mechanisms.

A technology such as WHART for instance provides authentication and encryption mechanisms such as AES 128-bit encryption at the network and transport layer from the data source to the data consumer. This is completed with integrity check measures aimed at ensuring that the message sent has not been modified or falsified and that the message is coming from the right source.

Despite those security mechanism, security holes are often created during the implementation phase in product. In February 2016, Applied Risk, an industrial control system security specialist revealed it had discovered several weaknesses in various WHART product

8.6 Main equipment manufacturers

The industrial communication market is very fragmented because of the presence of both local and global players. Well known players, all technologies considered are Voith, Mitsubishi Electric Corporation, Rockwell Automation, Yaskawa Electric Corporation, General Electric, Emerson Electric, Yokogawa Electric, Toshiba Machine Corporation, Honeywell International, FANUC Corporation, and ABB.

The table below provides a list of players by communication technology:

Table 33: Equipment manufacturers by industrial communication technology

Technology	Manufacturers
WHART / ISA100a	ABB, Emerson, Endress+Hauser, Pepperl+Fuchs, Siemens, Schneider Electric, GE, Dust networks, Endress+Hauser, CDS…
ISA100a	CDS, Rohrback Cosasco Systems, Yokogawa, GE, Murata, Spirax Sarco, Armstrong International, Honeywell, Bitherm, Flowserve, Riken Keiki, Cisco, Eltav, Yokogawa, GasSecure, Nexcom, SKF
WISA/WSAN	ABB

Source: IDATE

8.7 Which evolutions in the next five years?

It is currently difficult to estimate how those specific industrial technologies will evolve in the coming years as compared to less specific technologies such as WiFi, cellular, Bluetooth which benefit from a far stronger ecosystem. Because each industry and each company has to manage its historical assets, it is likely that those technologies will continue to be used with other technologies taking over only on a longer term.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

9 LPWA technologies

9.1 Synthesis

Table 34: LPWA technologies - synthesis

LPWA technologies	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	+ to ++ Will likely play a significant role; LoRa@2.4 GHz meets the industry requirements in terms of range, consumption and international capability
Description	Short to long range technologies aimed at connecting sensors & actuators. Can be used in the factory, mostly for monitoring, control, automation and analytics
Standards and regulatory constraints	ETSI is going to standard LPWA technologies LoRa Alliance for LoRa. Proprietary for SigFox, Ingenu…
Area of operation	Worldwide
Protocols used	See detailed descriptions below
Security	+
Performances	A few kbps
Range	10 m-20 km
Electrical consumption	Limited consumption of devices: up to 10 year battery life
Environmental aspects (ATEX, gas, temperature, CEM…)	?
Use sectors (public networks, industrial networks, future use for FoF)	Commercial networks, Industrial networks, FoF
Maturity (TRL)	TRL9
Availability & associated constraints	A fragmented market with a lot of competing technologies and very limited interoperability
Main providers	Chipsets: Semtech ST Micro
Price of equipment	Chipsets: $5 to 7 for LoRa, $2 for SigFox

Source: IDATE

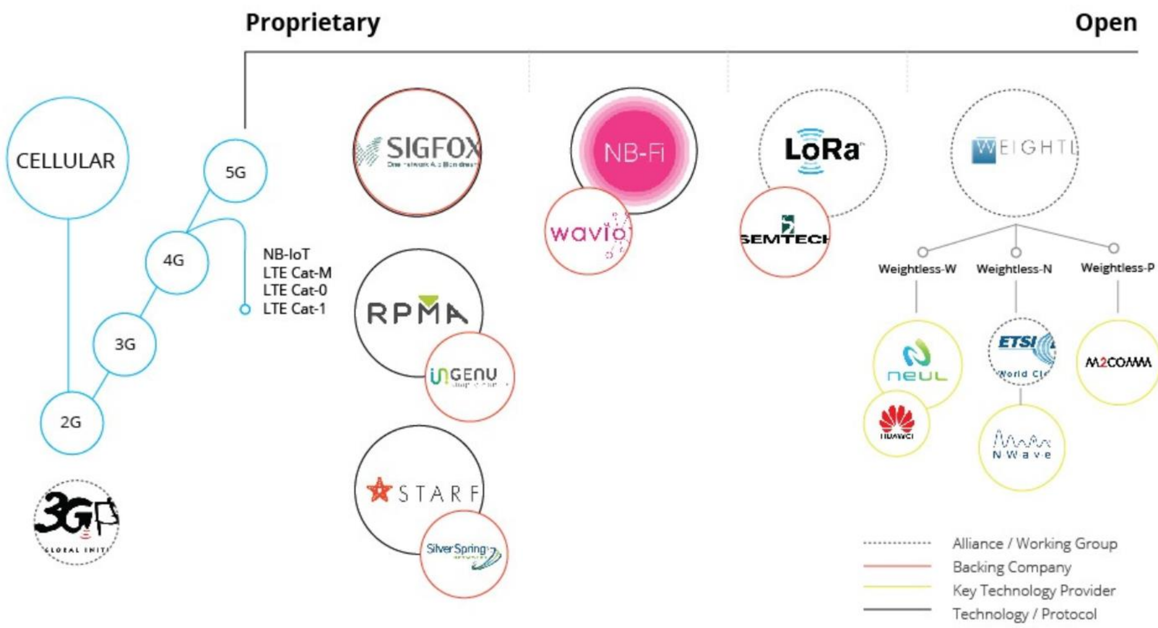
9.2 Performance of LPWA technologies

The Low-Power Wide Area (LPWA) technology is considered a new class of connectivity technology beside traditional cellular and wireless technologies. LPWA encompasses wireless connectivity technologies capable of delivering multiple years of device operation running on a single AA battery and able to cover wide areas of signal from the gateway to the devices, taking the environment into account. Generally, it has been designed to support devices

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

requiring small amounts of data transmission over medium or long distances, at low-power consumption and at low cost. Indeed, LPWA connects devices needing low bitrates in the IoT arena.

Figure 19: LPWA and wireless IoT technologies



Source: Postscapes

Table 35: Characteristics of LPWA

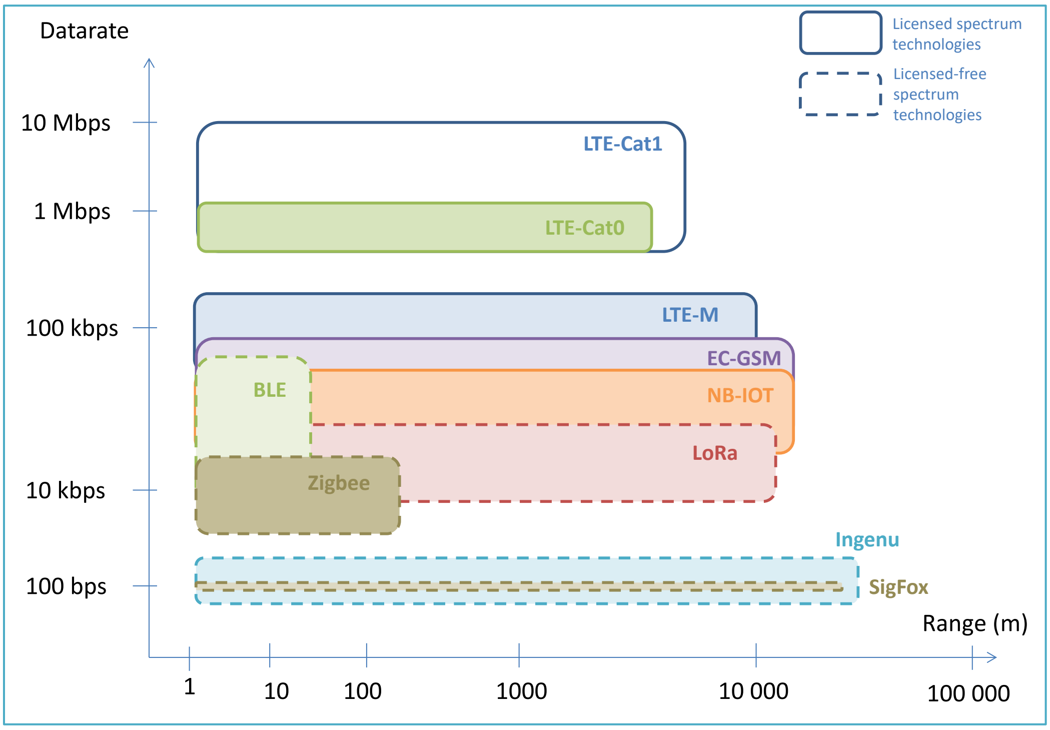
Characteristics	LPWA target
Range	2-40 km
Power autonomy	10-20 years
Bitrates	Few bps to hundreds kbps
Cost module	Few euros

Source: IDATE DigiWorld, *Key IoT technologies*, July 2017

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

In this report, LPWA is considered as using unlicensed spectrum while in the industry it could also encompass licensed spectrum.

Figure 20: Landscape of IoT/M2M networking technologies



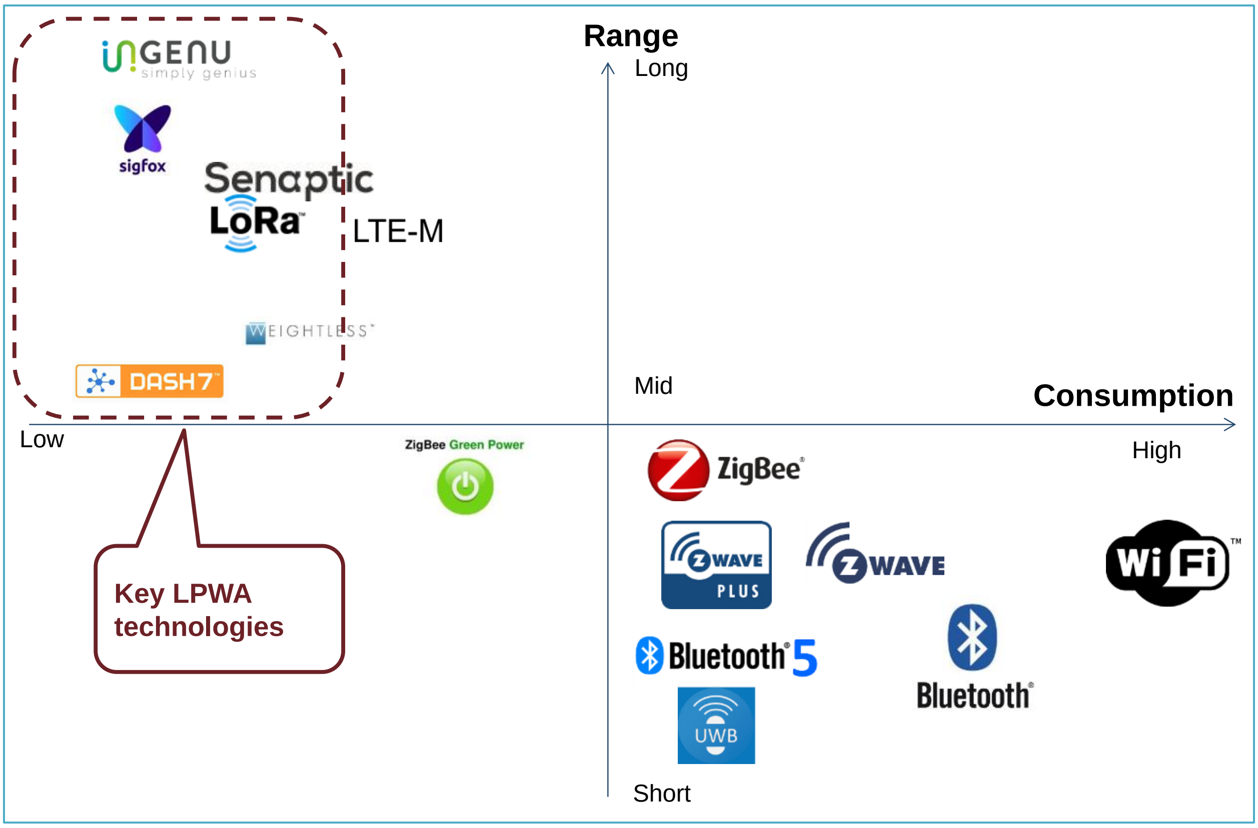
Source: IDATE DigiWorld, in *World M2M markets*, November 2016

LPWA operates in the ISM bands which are reserved internationally for the use of radio frequency energy for industrial, scientific and medical purposes other than communications. The ISM bands cover frequency bands recommended primarily for telemetry, alarms and data in general and other similar applications. The bands are unlicensed and could therefore be freely used but with some constraints (including power emission and duty cycle). Typically, simultaneous use (or noise or interference) on those band is limited. Consequently, technologies using ISM bands are not well suited to applications requiring service-level guarantees, such as availability, as in the case of driverless cars.

Today, more than 20 players provide LPWA technologies with LoRa and SIGFOX being the most popular but also including names like Ingenu, Senaptic and Weightless.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 21: LPWA technologies mapping of RF technologies in terms of range and consumption



Source: IDATE DigiWorld, *Key IoT technologies*, July 2017

The table below compares the specification of the main LPWA technologies:

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 36: LPWA technologies comparison

Technology	LoRa	SigFox	Weightless-N	Weightless-P	Senaptic	Ingenu	Cellular (NB-IOT)
Frequency band	868 MHz (EU) 915 MHz (US) 470 MHz (CHN)	868 MHz (EU) 915 MHz (US) 470 MHz (CHN)	868 MHz (EU) 915 MHz (US)	169/433/470/780/ 868/915/923 MHz	60/200/433/ 470/868/ 915 MHz	2.4 GHz	LTE bands
Interoperability	Proprietary	Proprietary	Standard	Standard	Proprietary	Proprietary	Standard
Battery life	+10 years	20 years	10 years	10 years	10 years	20 years	10 years
Bitrate	300 bps - 50 kbps	100 bps	100 bps	200 bps – 100 kbps	72.5 bps (UL)/500 bps (DL)	624 kpbs (UL) / 156 kbps (DL) 2 kbps in mobility	Tens of kbps
Mobility management	Yes	Yes	Yes	Yes	Yes	Yes	No
Two-way communications	Yes	Not really (kind of 2-way since mid-2015)	Yes/No	Yes	Yes/No option	Yes	Yes
Range	15 km in rural 2-5 kms in dense areas	Up to 40 km in rural areas	3 km in urban	2 km in urban	20 km rural 3 km in urban	48 kms	10-15 km
Transmission through thick walls	++	+	+	+	-	++	--
Footprint (geographical availbility)	28 countries on 4 continents	29 countries mainly in Europe	3 cities	Deployed ?	30 countries	Global but mainly US	Global

Source: IDATE

9.2.1 SigFox

SIGFOX has started implementing its proprietary technology in 2012 with a clear value proposition based on very low energy consumption (20 years battery life), low cost (2 USD) and large coverage. Indeed, based on ISM frequency bands, the range offered by SIGFOX can reach up to 40 km with a limited bitrate (100 bps), a limited payload at 12 bytes and high level of sensitivity.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Actually, the company positions as a telecom operator but not as a technology provider compared to other players studied in this section. SIGFOX interest is to provide global coverage indoors and outdoors. The lower spectrum is more used for outdoor environment whereas the 2.4 GHz is mainly used for city applications. Although 169MHz and 868 MHz are the bands currently used, SIGFOX is very independent with regards to frequency.

SIGFOX architecture also differentiates by the low antenna density. For instance, 1200 antennas are required to cover the whole France, expected to handle 10 billion objects. The company relies on satellite to connect the antennas to the cloud and 3G for back-up. For the hosting of telecom equipment composing its network, SIGFOX has concluded a partnership with TDF, a French company which provides radio and television broadcasting services. The TDF footprint (existing tower sites) increases the quality of service that SIGFOX is committed to providing its customers. Actually, SIGFOX claims it completed the French network rollout in 2014.

As regards to security, SIGFOX relies on a 128 bit AES authentication.

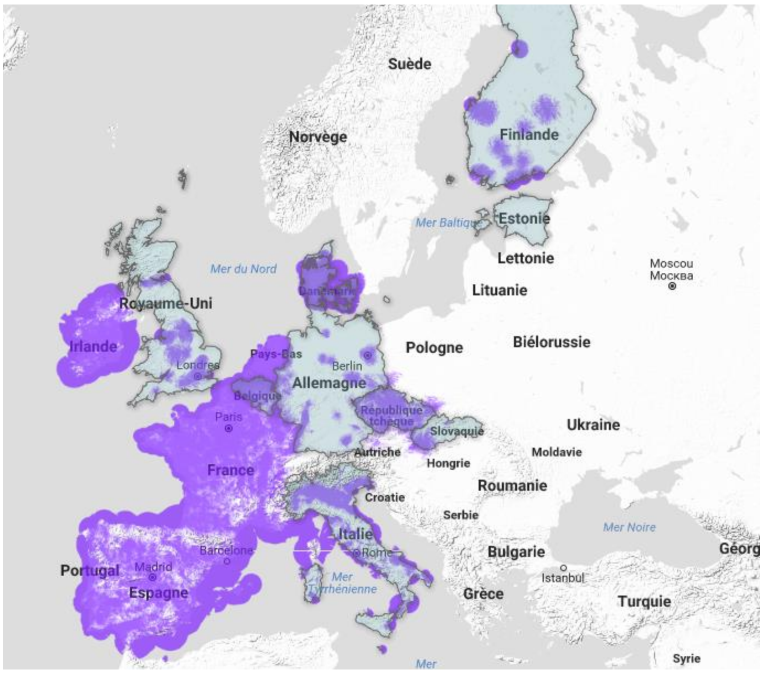
The targeted markets of SIGFOX include smart metering and tracking (alerts, water leakage, pallets…) for which the unidirectional connection is enough. SIGFOX has launched the bidirectional communication in 2015 but it does not correspond to a full 2-way connection.

For its development, SIGFOX builds national networks in countries it wants to address through exclusive partnerships with local players mostly as part of SIGFOX Network Operators. Some of them are also shareholder of the company such as Telefónica and Engie.

In terms of deployments, SIGFOX is present in 29 countries as November 2016 and has registered 10 million modules. The company plans to cover 50 countries by 2019.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 22: SIGFOX coverage in Europe



Source: SIGFOX

9.2.2 LoRa

LoRa which stands for Long Range is a technology solution acquired by the chipset maker Semtech in 2012. This proprietary solution is especially exploited for its significant long range capability improved by spectrum modulation technique. The main benefits of the technology using the ISM frequency bands are the range reaching up to 15 km in rural areas, the deep indoor penetration and the low energy consumption of devices. In addition, the payload can be configurable on the fly from 0 to 256 bytes with an optional 128-bit AES encryption. The targeted applications cover especially smart metering, sensors network and smart cities.

LoRa is notably used in LoRaWAN (Long Range Wide-Area Network), a low power network protocol designed for wireless battery operated things in a regional, national or global network.

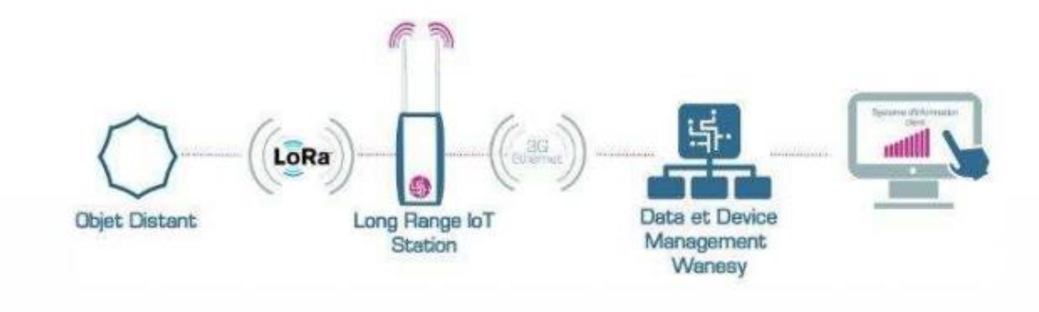
Also, the particularity of LoRa is the ecosystem behind thanks to LoRa Alliance jointly founded by LoRa and Semtech. LoRa Alliance is constituted of members with the mission to standardise and collaborate to drive the success of LoRaWAN, by knowledge and experience to guarantee interoperability between operators in one open global standard. The idea is to make LoRaWAN a de facto standard in the near future.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Actually, LoRa Alliance members embed LoRa technology in addition to the traditional licensed cellular technology. Unsurprisingly, the alliance is mainly composed of mobile carriers which decided to integrate the LoRa technology into their portfolio to address new applications and businesses such as Bouygues Telecom, KPN and Swisscom. Some telcos are also embracing LoRa technology even without becoming member of the Alliance: this is the case with Orange. However, the LoRa Alliance is also composed of industrial and M2M / IoT solution providers along the technical chain.

Thus, LoRa has already numerous commercial references with the deployments of the technology by mobile operators as part of LoRa Alliance totalling 10 million modules which base is keeping growing. For instance, SK Telecom (which is a key stakeholder in SIGFOX and also a member of the LoRa Alliance) expects to connect over 4 million devices to the IoT dedicated network by the end of 2017. LoRa has also be retained for smart metering project like m2ocity (Orange) but also for a large smart meter deployment in Russia involving 400 000 smart meters.

Figure 23: Principle of LoRa



Source: LoRa Alliance

9.2.3 LoRa @ 2.4 GHz

LoRa @2.4 GHz is an evolution of the LoRa technology with the objective to use the unlicensed 2.4 GHz band and to provide longer ranges. In France, Altran is integrating an implementation of the technology for industrial companies such as Arkema, Areva, Total, Ariane …

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Table 37: LoRa@2.4 GHz

LoRa @ 2.4 GHz	Evaluation of the technology
Future role of the solution in the industry	+ The energy sector in France is interested by this technology, especially for use in nuclear plants
Description	Compared to the LoRa Wan protocol, LoRa@2.4GHz has no duty cycle limitation and works in both synchronous and asynchronous modes. A dedicated coding is used in order to provide better interference protection and longer range. Radio channels are narrower than WiFi channels and the 2.4 GHz band has the advantage (over sub-1 GHz unlicensed bands) to be available all around the World. It is also possible to have a very good indoor penetration (because the protocol used is more deterministic than in LoRaWAN) and to perform indoor and outoor geolocation. A Semtech Chipset (as for LoRa Wan) is used by Altran with a dedicated radio module (provided by Idosens) for the 2.4 GHz band.
Standards and regulatory constraints	LoRa@2.4 GHz is fully standard (LoRa Alliance)
Area of operation	Industrial environment
Protocols used	LoRa: PHY layer; LoRaWAN: MAC, NWK, & APP built on LoRa
Security	Fully secured with dedicated software (confidential)
Performances	270 kbps both uplink and downlink Up to 2 MByte par device per day Coverage in challenging environment (metal): one gateway for 10000 m² Geolocation can be performed by dedicated beacons: small antennas which measure propagation delay of the signal. Possible to realise triangulation for both indoor and outdoor geolocation
Range	20 km. According to Altran, it is possible to go up to 80 km in straight line and with no water or foliage.
Electrical consumption	Depends on the environment : up to 5 years for one message per day
Environmental aspects (ATEX, gas, temperature, CEM…)	Some products are currently about to get ATEX certification AREVA and Total are asking for ATEX products
Use sectors (public networks, industrial networks, future use for FoF)	Industrial environment, asset tracking for indoor location, asset management (but also remote control capability), predictive maintenance, ability to be integrated in very constrainted environments, real-time upload
Maturity (TRL)	TRL 8: now being industrialised
Availability & associated constraints	The chipset provider Semtech provides both Lora WAN and LoRa@2.4GHz chipsets
Main providers	In Asia, many companies are currently developing LoRa@2.4 GHz for asset tracking
Price of equipment	N/A

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

9.2.4 Ingenu

Formerly named On-Ramp Wireless and founded in 2008, Ingenu is a US-based company that has developed RPMA (Random Phase Multiple Access) technology mainly characterized by a large and deep coverage that limits the need of infrastructure. Actually, RPMA network utilizes the unlicensed spectrum 2.4 GHz band and covers up to 450 square meters (~1200 km²). Ingenu claims to support up to 2 million devices per tower. RPMA is also designed and optimized for deep coverage penetrating underground (1 mile in depth), through concrete and inside dense buildings. The technology provides a full two-way data flow with flexible frame sizes varying from 6 bytes to 10kbytes and a long battery life of 20 years.

High level of security is also key features of Ingenu network with 256 bit AES authentication but also with other specifications like device anonymity, mulitcast authenticity and authenticated firmware upgrades.

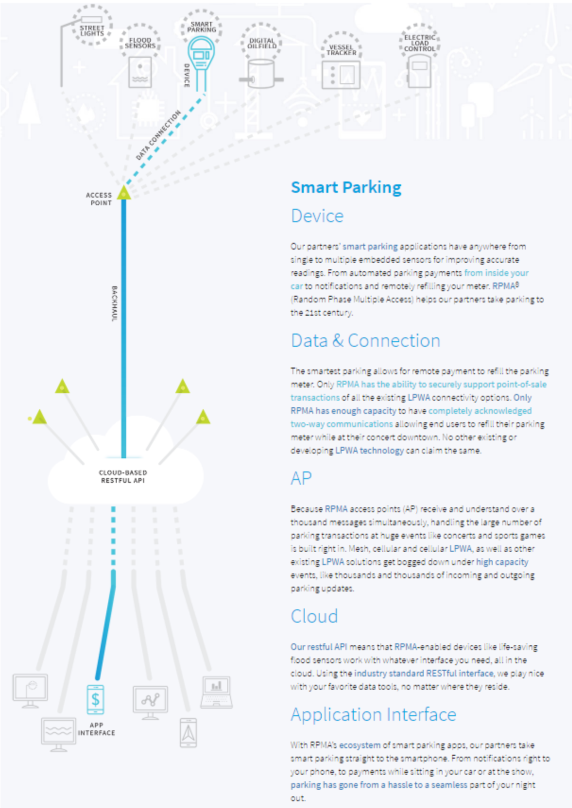
Regarding interference in the 2.4 GHz, RPMA has been designed to support the high level of noise with adapted receiver sensitivity.

There are broad potential applications but Ingenu targets applications such as smart cities, tracking and environment monitoring.

Ingenu network is built by the company and its partners. In fact, RPMA can be deployed in both public and private networks, the company is currently building a public LPWA network in the US named the Machine Network with a targeted 100 major metropolitan areas covered by the end of 2017. Aside, Ingenu already available in Japan, Chile, Nigeria, the Dominican Republic and Canada is planned to be expanded in Europe. Actually, Meterlinq, an Italian telemetry company is using Ingenu in its smart metering services for business and residential gas meters.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Figure 24 : Application of Ingenu for smart parking



Source: Ingenu

9.2.5 Senaptic (Telensa)

Created in 2014, Senaptic is a UK company and a spin out of Plextek. The radio technology used by the company called Ultra Narrow Band (UNB) has been designed for over the last 15 years and deployed in more than 30 countries. Senaptic's business model is about building a global network from local licensees for which they provide network equipment, software and connectivity. The technology is deployed around the world and counted 8 million active devices in 2016.

The technology mainly addresses utilities, smart homes and smart cities verticals and applications such as water metering, vehicle tracking, parking guidance, environmental monitoring and street lighting. Senaptic benefits from a strong presence in smart street lighting thanks to a major agreement with Telensa, a key player in the field. 10% of UK street lights are based on UNB technology.

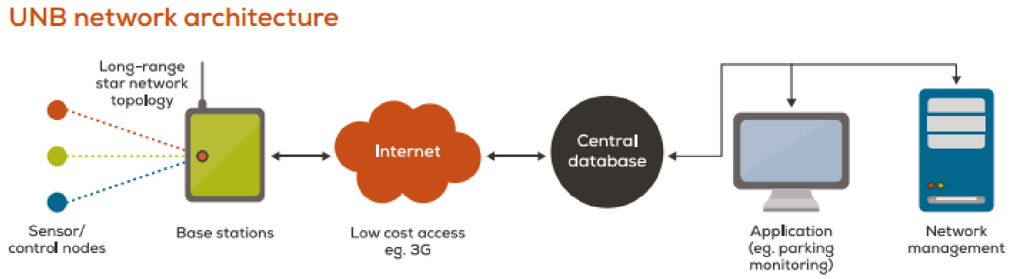
UNB combines long range with ultra low energy requirements, reducing the number of base stations required to cover an area. Indeed, the RF technology typically achieves a range of 20km in rural areas and 3km in urban areas with battery life running up to 10 years (6-7 years for some application use like parking monitoring). As an example, 33 base stations currently cover Birmingham, a 1 million population city in the UK.

Two connexion modes are available bidirectional in which data transfers are acknowledged, and uplink only providing longer battery life. UNB is also optimised for low bandwidth transmissions at 72.5 bps in uplink and 500 bps in downlink.

The system can operate in licence-exempt spectrum (868 MHz in Europe, 915 MHZ in the US, 470 MHz in China) but can also be adapted for use across a range of dedicated bands (60 MHz et 200 MHz).

As regards to Senaptic architecture, UNB utilises a network configuration where each base station is able to communicate with many thousands of sensor nodes, typically 5000 devices per base station.

Figure 25: Principle of Senaptic Ultra Narrow Band architecture



Source : Senaptic

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

10 Mesh network technologies

10.1 Synthesis

Table 38: Mesh network technologies - synthesis

Mesh network technologies	Evaluation of the technology
Future role of these solutions in the industry/evolutions of the technology in 5 years	- No likely role in the short to medium term
Description	Radio communication networks in which radio nodes provide retransmission capabilities to neighbouring nodes, allowing end-to-end connectivity in the network based on multi-hop routes
Standards and regulatory constraints	IEEE working group 802.11s
Area of operation	Worldwide
Protocols used	Under development
Security	Unknown
Performances	Likely up to a few Mbps
Range	Short to long range (up to 20 km)
Electrical consumption	Google WiFi router: comparable to other WiFi routers
Environmental aspects (ATEX, gas, temperature, CEM…)	Unknown
Use sectors (public networks, industrial networks, future use for FoF)	Commercial networks, Industrial networks, FoF
Maturity (TRL)	TRL 9
Availability & associated constraints	Unknown
Main providers	Unknown
Price of equipment	Google WiFi Router: $200-300

Source: IDATE

10.2 Performance of mesh network technologies

Mesh networks are radio communication networks in which radio nodes provide retransmission capabilities to neighbouring nodes, allowing end-to-end connectivity in the network based on multi-hop routes. There are two main categories of mesh networks:

- 'Structured mesh networks': in which the radio nodes have fixed positions
- 'Ad-hoc mesh networks': in which the radio nodes act as mobile terminals

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

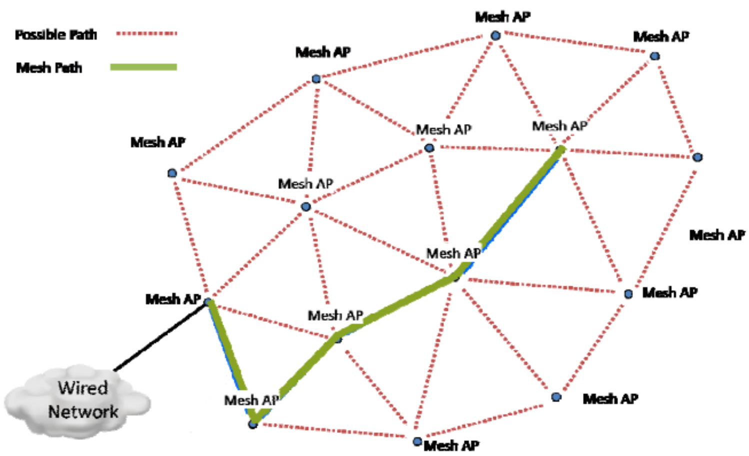
10.2.1 Structured mesh networks

The term 'mesh network' (in the meaning of structured mesh network) is often used in relation to Fixed Wireless Access (FWA) systems which are applied to provide access services to small and medium enterprises, home offices and residential users.

Common FWA systems are based on a Point-to-MultiPoint (P-MP) architecture, in which a base station serves several fixed terminal stations within its service area. Each base station can be equipped with a single omni-directional antenna or, more usual, multiple antennas each serving a separate sector (e.g. 90º or 60º wide). To each base station one or more frequency channels are assigned (depending on the number of sectors). By installing multiple base stations a larger area can be covered, in a similar way as is done with cellular networks for mobile communications.

(Structured) Mesh networking is in fact an extension of the FWA concept in which terminals are equipped with the functionality to directly communicate with other terminals within their reach, i.e. ignoring the base station. The terminals are able to relay their transmissions, so a meshed communication network is formed as schematically shown in the figure below**Erreur ! Source du renvoi introuvable.**:

Figure 26: Schematic representation of a mesh network



Source: CWNP

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

10.2.2 Ad-hoc mesh networks

Ad-hoc mesh networking is based on mobile terminals and/or devices which form an autonomous network as they come into each others vicinity. Ad-hoc networking functionality pursues a high level of self management and self healing functionalities and minimal requirement for intervention of the users or a network operator. Within the ad-hoc networking framework several network management protocols are defined e.g. to admit additional terminals which come in range of the other network nodes protocols, to optimise transmission power levels, and update route selection algorithms to improve the overall transmission efficiency.

The self organising and automatic network management features make ad-hoc networks easy to use and convenient in many applications:

- Personal Area Networks (PAN): interconnection of devices in the home environment such as TV, PC, organiser, mobile phone, video recorder;
- (Temporary) Local Area networks: for instance at conferences, exhibitions or business meetings;
- Mobile communications;
- Sensor networks: communication between intelligent sensor devices;
- Robotics: swarms of wirelessly interconnected robots or similar 'mobile autonomous systems'
- Communications for military and public safety operations: fast connection establishment in areas where no communication infrastructure is present or communication means are damaged;
- Communication between vehicles: for intelligent transport systems, safety increasing applications or to provide road-side information

10.2.3 Benefits of mesh networks

Mesh networking can offer benefits compared to the more commonly applied cellular network topologies based on the deployment of base stations in central network management. The most important benefits of mesh networks are listed below:

- No single point of failure

  In cellular networks the base station forms a critical factor in the communication infrastructure. When the base station fails all communication within that cell is disrupted. In mesh networks terminals the nodes on which the communication is based and there is no dependence on a base station. If one node fails, this will have just a limited performance effect on the total mesh network.
- Robustness due to alternative routing possibilities in the network

  Terminals are nodes in the mesh network and are able to route the data traffic through the network. Communication between terminals is possible even if they do not have a direct connection, as long as there is a path through the network (formed by terminals relaying the transmission) along which the transmission can be routed. As the density of nodes (terminals) increases, multiple paths in the mesh network may be created along which the traffic can be routed, which increases the robustness of the end-to-end connection. When a certain radio link between two terminals is interrupted, in a dense mesh network there often will be an alternative path along which the traffic can be routed so that communication is still possible.

- Range extension and coverage enhancement

  At the very high frequencies that are used for broadband communications nowadays, the range of radio links attainable is limited. Mesh networks may be used to extend the range of base stations in a cellular network. In this case mesh networking terminals (just) within the coverage area of a base station are used to relay transmission to terminals that are beyond the range of the base station. This way the coverage are of a cellular network can be extended without the direct need for deploying additional base stations.

  Another effect related to the use of very high frequencies is that obstacles in the radio path, such as buildings and trees, result in a significant attenuation of the radio signal. Therefore many broadband radio systems require a (nearly) free line of sight between base station and terminal (in a cellular network) or between individual terminals in a mesh network in order to establish reliable communication links. In a cellular network it often occurs that many geographical locations that fall within the theoretical range of a base station can not be served due to signal blocking caused by obstructions in the radio path. With the relay function in mesh networks the coverage can be significantly be improved as the radio signal can be diverted around obstacles by relayed from terminal to terminal. This coverage improvement is considered as a significant benefit of mesh networking, which applies under the condition that there is a sufficient number of terminals within the mesh network.

The benefits specifically related ad-hoc mesh networks are the following:

- No fixed installed infrastructure;
- Networks are self organising;
- There is no need for network planning.

10.2.4 Technical challenges in mesh networking

The dynamic network topology (terminals moving within, joining and leaving the network) and realising efficient and reliable multi-hop communication are the basic challenges for mesh ad-hoc networking. An additional complicating factor is the distributed nature of mesh ad-hoc networks, where there is no central management entity controlling the network, but networking functionalities are distributed among the nodes. Nowadays research is aimed at solving these challenges for mesh ad-hoc networking and optimising communication possibilities offered by these networks.

Besides the benefits that can be offered by (ad-hoc) mesh networking there are also a number of issues to be resolved. The most important issues are:

- Transmission delay in the network when in case of routing along multiple hops;

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

- Optimisation of routing protocols,
  Realising fairness among the network nodes;
  To offer end-to-end quality of service guarantees;
  To support terminal mobility of nodes within mesh networks;
- Scalability,
  High node densities
  Effective data throughput deterioration in case of much transit traffic;
  Spectrum reuse; tackling interference;
- Security,
  Authentication;
  Admission control;
  Information security;
- Increased terminal costs;
- Willingness to relay.

10.3 IEEE 802.11s: adding mesh capability to WiFi networks

IEEE 802.11s corresponds to the Wireless LAN standard for mesh networking, and defines how wireless devices can interconnect to create a WLAN mesh network. It is a IEEE 802.11 amendment.

The IEEE working group 802.11s initiated a project for the standardisation of Extended Service Set (ESS) Mesh, also called WiMesh. The objective is to specify an extension of the existing 802.11 (WLAN) standards for an interoperable solution to enable self-organising multi-hop network topologies.

The purpose of the project is to provide protocols for auto-configuring paths between nodes in a multi-hop mesh network. The mesh functionality is initially designed to provide additional functionality as an extension to the existing WLAN and WiMAX standards. Mesh functionality will therefore be available in local area applications and in broadband access networks.

The IEEE 802.11s working group started its activities in 2005 and hoped to produce an approved standard in 2008. In June 2011 the fifth recirculation Sponsor Ballot, on TGs Draft 12.0, was closed. The 2012 release of the 802.11 specification (802.11-2012) directly incorporates Mesh Routing functionality. Besides introducing wireless frame forwarding and routing capabilities at the MAC layer, the 802.11s amendment brings new interworking and security.

An example of IEEE 802.11s implementation is the Google Wifi router which is is a mesh-capable wireless router. It was announced on October 4, 2016, and released in the United States on December 5, 2016. Further international

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

rollout followed, with the United Kingdom on April 6, 2017, Canada on April 28, 2017, France and Germany on June 26, 2017, and Australia on July 20, 2017. Google Wifi aims to provide enhanced Wi-Fi coverage through the setup of multiple Wifi devices in a home. Wifi automatically switches between access points depending on signal strength. Wifi can be purchased as a single unit or in a multi-pack. One Wifi device looks like a little white cylinder. For the technical aspects of its functionality, Wifi features 802.11ac connectivity with 2.4 GHz and 5 GHz channels, 2x2 MIMO antennas, and support for beamforming. It has two gigabit Ethernet ports, and contains a quad-core processor with 512 MB RAM and 4 GB flash memory. Wi-Fi access can be controlled through a companion mobile app. This router is dedicated to the residential market and has no customization capabilities necessary for the enterprise market.

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

11 Sources

Private LTE&5G for industrial IoT (Qualcomm) Mehmet Yavuz

Profibus : pxddamkey[8477]_2010-_C10_-_Stabilisation_of_wireless_profibus-_Thomas_Schildknecht

HCF : HART Wireless Brochure v10 Final

HCF : WirelessHART Security Overview

ABB : A-Vallestad-WISA_becomes_WSAN-Wireless-Summit-2012

ABB : introduction to WISA

Unibs.it : Wireless Sensor Networks for Industrial Applications

frostsullivan-whatshotintheindustrialautomationandprocesscontrolindustry-120528075056-phpapp01

Sepura : A comparison of TETRA and GSM-R for railway communications

DMR Association : benefits of DMR

TCCA : Mobile Broadband in a Mission Critical Environment

TCCA : TETRA versus DMR

Federal Office of Communications OFCOM (CH) : Tetrapol Factsheet Trunked radio system for emergency services

IHS: The Future of Wireless In Industry Remote 2013 Tom Moore – Analyst, Discrete Automation

National Institue of Standards and Technology : LTE Security – How Good Is It?

Technische Universitat Berlin ¨Telecommunication Networks Group : Power consumption of WLAN network elements

Analysys Mason DMR Market Report (2011)

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

WISA:
http://www.millennialnet.com/MillennialNet/media/Resources_Media/WhitePapers/WhitePaper_IntroductiontoWISA_V2.pdf

IDATE studies:

- Industrial Internet (2017)
- IoT (2017)
- LTE Watch Service (2010-2017)

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

12 Glossary

Acronym	Meaning
3GPP	3rd Generation Partnership Project International organisation in charge of UMTS and LTE standardisation
Bluetooth	
CAPEX	Capital Expenditures
CDMA	Code Division Multiple Access
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
C-RAN	Cloud or Centralised RAN
D2D	Device to Device
DL	Downlink
DMR	Digital Mobile Radio
eMBB	eMobile Broadband
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Duplex
GPRS	General Packet Radio System. Evolution of GSM enabling packet instead of circuit mode transmission
GSM	Global System for Mobile communications
HetNet	Heterogeneous Networks
HomeRF	
HSDPA	High Speed Downlink Packet Access, an evolution of WCDMA technology
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
kbps	Kilobits per second (unit for measuring data speeds)
LoRa	Long Range
LTE	Long-Term Evolution
MAN	Metropolitan Area Network
Mbps	Megabits per second (unit for measuring data speeds)
MIMO	Massive Multiple-Input, Multiple-Output
MNO	Mobile Network Operator
M2M	Machine to Machine
NFC	Near Field Communications
OFDM	Orthogonal Frequency Division Multiplexing
PMR	Professional (Private) Mobile Radio
QAM	Quadrature Amplitude Modulation, a modulation technique

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr

Acronym	Meaning
R&D	Research&Development
LTE-V2X	LTE-Vehicle to Everything
QAM	Quadrature amplitude modulation
RAT	Radio Access Technologies
RFID	Radio Frequency Identification
SON	Self Organising Network
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
UL	Uplink
UMTS	Universal Mobile Telecommunication System. Third generation cellular telephony norm, standardised by the 3GPP
uRLLC	ultra Low Reliable Low Latency Communications
UWB	Ultra-Wide Band
VLC	Visible *light* communication
WCDMA	Wideband CDMA. Radio interface selected for UMTS, enabling speeds of several hundred kilobits per second
WiFI	WLAN technology standardised in the US. WiFi is the most highly developed and most mature of all WLAN technologies (www.wi-fi.com)
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability Microwave Access. What is commonly called WiMAX is associated with the IEEE 802.16a, 802.16REVd and 802.16e
WISA	Wireless Interface to Sensors and Actuators
WLAN	Wireless Local Area Network. Includes several norms: 802.11b (also known as WiFi), HomeRF, HiperLAN 2 and 802.11a
WPA	Wi-Fi Protected Access

NORMANDIE AEROESPACE
Technopôle du Madrillet
745 avenue de l'Université - Bâtiment CRIHAN
76800 Saint-Etienne du Rouvray
T +33 (0)2 32 80 88 00
www.nae.fr