International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(2020)

FG-NET2030 – Focus Group on Technologies for Network 2030

FG-NET2030-AddCases

Network 2030 – Additional representative use cases and key network requirements for Network 2030

Summary

Towards the year of 2030 and beyond, many novel applications are expected to emerge as others mature, leading to increasingly intertwined human and machine communications. New applications often trigger new services and introduce challenging requirements that demand the continuous evolution of networking technologies. Thus, the inherent capabilities of interconnected networks and the running principles therein need to be enhanced, or even replaced, as requirements unfold.

To help identify the essential network requirements and shape the future networks' design paradigm, this report continues working on representative use cases for Network 2030 that have been selected through group discussions within Sub-Group 1 of the ITU-T Focus Group on Network 2030 (FG NET-2030).

Specifically, this report covers five additional use cases to those contained in the previous report [34]: Huge Scientific Data Applications, Application-aware Data Burst Forwarding, Emergency and disaster rescue, Socialized Internet of Things, and Connectivity and sharing of pervasively distributed AI data, models and knowledge. Their corresponding key network requirements are also briefly stated.

Finally, it is important to note that additional use cases and further details on those presented can be found in the global set of contributions submitted to the ITU-T FG NET-2030 and are accessible in the SharePoint repository 0.

History: All historical documents are in Sub-G1 SharePoint (https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/SitePages/Sub-Group%201.aspx).

Keywords

Network 2030, use cases, network requirements

NOTE

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

FG NET2030 Technical Report on

Network 2030 – Additional use cases and key network requirements for Network 2030

Scope of this report

In **Part I**, five representative use cases with their key network requirements are presented:

- Huge Scientific Data Applications;
- Application-aware Data Burst Forwarding;
- Emergency and disaster rescue;
- Socialized Internet of Things;
- Connectivity and sharing of pervasively distributed AI data, models and knowledge.

Then, in **Part II**, five overarching abstract requirement dimensions (articulated within each use case in part I with respect to their related requirements) are compared graphically. The representative use cases are also briefly analysed from the abstract requirement dimension perspective.

Abbreviations and acronyms

This technical report used the following abbreviations and acronyms:

ABF	Application-aware data Burst Forwarding
CERN	Conseil Européen pour la Recherche Nucléaire
CSAI	Connectivity and Sharing of pervasively distributed AI
EDR	Emergency and Disaster Rescue
FAST	Five-hundred-meter Aperture Spherical radio Telescope
HSD	Huge Scientific Data applications
ICT	Information and Communications Technology
IP	Internet Protocol
LHC	Large Hadron Collider
MSIC	Mass Service of Individualized Control
MTU	Maximum Transmission Unit
NIC	Network Interface Card
PCN	Public Communication Networks
QoS	Quality of Service
SIoT	Socialized Internet of Things
SKA	Square Kilometer Array
STIN	Space-Terrestrial Integrated Network
TCP	Transfer Control Protocol
TDMA	Time Division Multiple Access
UAV	Unmanned Aerial Vehicle
VLBI	Very Long Baseline Interferometry
WRR	Weighted Round Robin

Part I: Use cases and network requirements

I.1 Huge scientific data applications (HSD)

I.1.1 Introduction to HSD applications

Looking back through the history of computer networks, the world's first network, ARPANET (Advanced Research Project Agency Network) was invented to support requirements of military and scientific research. The World Wide Web (WWW), invented by Physicist Tim Berners-Lee in 1989 while working at Conseil Européen pour la Recherche Nucléaire (CERN), was initially conceived and developed to meet the demand for automated information-sharing between scientists in universities and institutes around the world. These revolutionary developments highlight and indicate that the requirements of scientific research often drive development of computer network technologies.

Large-scale scientific applications, such as astronomical telescopes, colliders, etc., play a critical supporting role in the development of human science and technology. Large-scale scientific experiments and observations produce vast amounts of data. With the development of network technology, scientific data flows are increasing rapidly expanding as is legacy Internet traffic, but scientific data flows have different characteristics in terms of quantity and scale. Compared with ordinary Internet application traffic, a scientific data flow could be considered an elephant in comparison to a mouse.

Depending upon the application a combination of elastic bandwidth and latency demands may be required. For example, different astronomical telescopes have individual configurations, such as decentralized global deployment and ground satellite communications. In this example, data needs to be transferred synchronously and processed simultaneously, which places strain upon communication links.

In another example, various particle accelerators and colliders could generate a massive amount of data within very short time periods; another example would be ITER – "the way" fusion experiment – which can generate data at 100GB/s. The rapid collection and transmission of this present numerous challenges.

The bandwidth demand for massive scientific data transfer has reached 100 Gbps and will reach Tbps in the future. Current networks cannot support such massive data transfer. For some scientific applications, the transfer of scientific data is still carried out in a conventional way such as disk or cassette.

Some examples of large-scale scientific applications are:

a) Astronomical telescopes

– **VLBI – Very Long Baseline Interferometry [2]**

VLBI enables astronomists to observe the starry sky. As Figure 1-(b) shows, a typical E-VLBI system consists of multiple distributed networked telescopes and a central correlator. Each telescope generates massive volumes of data continuously, and this data needs to be transferred to the correlator in real-time. The VLBI produces 256Mbps~16Gbps per site and is only set to increase.

– **SKA – Square Kilometer Array [3]**

The SKA is an array of radio telescopes made up of thousands of smaller dishes. This next generation of Radio Astronomy Observation Facility will collect and handle about 130-300 PB of data per year.

– **FAST – Five-hundred-meter aperture spherical radio telescope [4]**

Five-hundred-meter aperture spherical radio telescope (FAST) is the largest single dish radio telescope in the world. It is now in the early stages of exploration and has varying requirements for its operation in different modes. In the simple mode, the amount of data generated is about 6 Gbit/s. This telescope's annual observable time is about 2800 hours, which means that the amount of data it generates will be as high as 60 PB per year. In the complex mode, data is produced at about 38 Gbit/s.

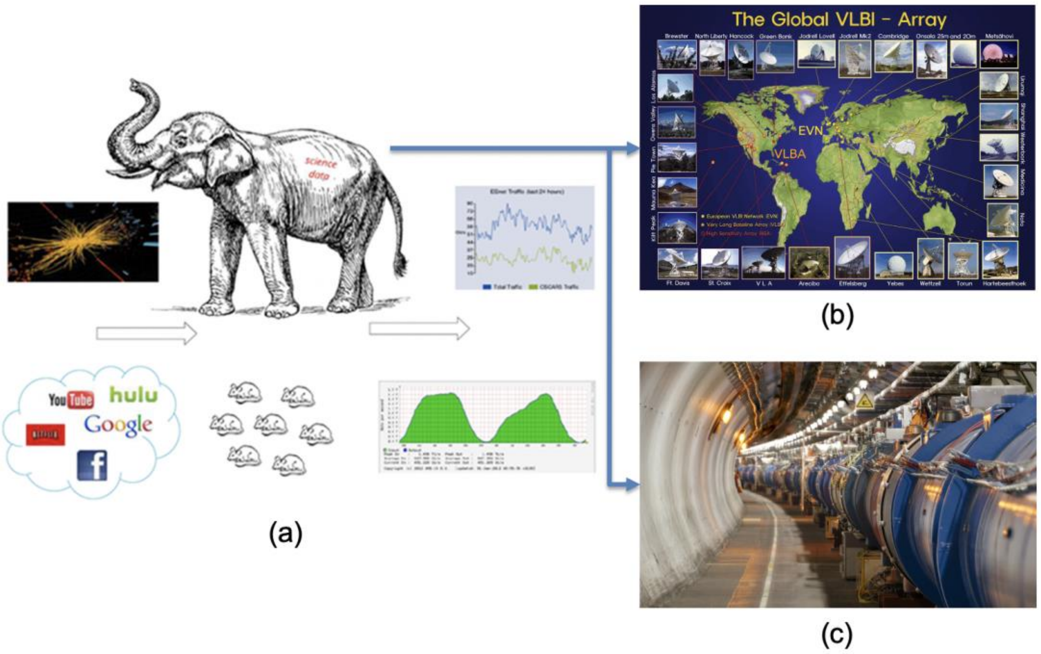


Figure 1 – (a) Comparison between huge scientific data application and general Internet application

b) Accelerators

– LHC – The Large Hadron Collider [5]

LHC is the world's largest and most powerful particle accelerator. It consists of a 27-kilometre ring of superconducting magnets, as shown in Figure 1-(c), and its data collection rate is around 40 Tbit/s.

c) Others

– ITER – "The Way" in Latin [6]

ITER is the world's largest tokamak and has been designed to prove the feasibility of fusion as a large-scale and carbon-free source of energy based on the same principle that powers Sun and stars. The ITER Front-end devices can source data at 100 Gbit/s.

The simple table below provides additional information about other huge scientific data applications in Table 1.

Table 1 – Requirements of applications

Huge Scientific Data Applications	Network Requirement	Store Requirement	Computing Requirement
High repetition frequency X-ray free electron laser device	10 Gbit/s	100 PB	1-10 PF
Shanghai Light Source Phase II	1 Gbit/s	500 PB	20-40 PF
BESIII	100 Gbit/s	15 PB	10 PF

Table 1 – Requirements of applications

Huge Scientific Data Applications	Network Requirement	Store Requirement	Computing Requirement
JUNO	100 Gbit/s	30 PB	10 PF
Major marine science and technology infrastructure	quantum encrypted communication	0.5 EB	100 PF

I.1.2 Key network requirements

It is clear from the above, that present transfer networks will not be capable of transferring the vast amounts of data produced by scientific applications in a timely manner. Additionally, there are several other challenges that need to be considered in the design of scientific data transfer networks.

– ***Bandwidth***:

The demand for transfer bandwidth for mass scientific data has reached 100 Gbps and will soon reach the order of Tbps. There is theoretically an unlimited demand for network bandwidth, because the observation of the universe is unlimited.

– ***End-to-end on-Demand QoS***:

In a distributed workflow system, the loss of one node will affect the whole workflow system, so each node needs an end-to-end guarantee. At the same time, different research applications require different scales of bandwidth, which can be minutes, days, or long-term. Take FAST as an example, the data generation rate in complex mode is about 38 Gbit/s, which is more than 6 times that of simple mode. The network should have the ability to provide bandwidth and resource allocation dynamically for effective utilization. The end-to-end dedicated bandwidth should preempt background traffic as well as guarantee the transfer of scientific data.

– ***Synchronization***:

Many scientific devices usually collect and transmit data to a remote processing center for real-time analysis during observation. For example, during e-VLBI observation, the data is continuously collected by multiple radio telescopes distributed at different locations. The delay of one node’s flow will result in the delay of the analysis result. For some observations, for example, when using e-VLBI observation for locating the spacecraft, the analysis result is needed in real-time. Therefore, the data should be synchronously transferred to the processing centre. On the other hand, the telescopes minimal local storage, and continuous data gathered must be transferred in real-time to remote storage nodes, or data will be lost.

– ***Reliability***:

The local storage size of scientific applications is usually small or even non-existent, which makes it challenging to retransmit lossy data, so the reliability of the link is crucial. Thus, the transfer link of scientific data requires a high-quality guarantee, such as low packet loss rate, low latency and low jitter. For example, the ITER nuclear fusion experiment runs 5-7 days a week and 8-16 hours a day. During the experiment, the network failure time cannot exceed 1 minute, requiring the network to have 99.999% availability [7]. As another example, the LHC data transmission lasts 9 months per year and can tolerate only a few hours of interruption, requiring a network availability of 99.95% [8].

– ***Protocol considerations***:

The traditional Transfer Control Protocol/Internet Protocol (TCP/IP) protocol suite has difficulties in supporting the timely transfer of these scientific data. The best effort transmission and the domain name resolution of the current IP protocol can be improved. For scientific data networks that have extremely high requirements on network quality and reliable transmission, some functions should be designed to guarantee service quality. For long-distance distributed scientific applications, it should be considered changing the addressing mode of the IP protocol to content addressing. For the congestion control algorithm of the transport protocol, it should be considered adding more link layer and physical layer parameters, such as delay and buffer congestion, to speed up the response to changes in channel status.

Future scientific applications, especially for large scale scientific projects, put forward significant challenges for networks, such as Tbps grade long-distance transfer rate, high reliability, deterministic delay and intent-based provision. These are practical requirements for future networks and motivations for the development of future network technologies.

I.1.3 Evaluation of the abstracted requirement dimensions

The scores below are given by the contributor based on the analysis of network requirements of the use case.

Bandwidth: 10; Time: 9; Security: 6; Artificial Intelligence (AI): 6; ManyNets: 9

(Note that all the scores are given according to the relative importance of a specific network requirement: 1 to 3 are for relatively LOW requirement; 4 to 6 are for MEDIUM requirement; 7 to 9 are for relatively HIGH requirement; and 10 means EXTREMELY demanding requirement)

I.2 Application-aware data burst forwarding (ABF)

I.2.1 Background and introduction

Burst forwarding is an application aware data forwarding technology that aims to optimize end system performance. It minimizes the end to end application data transmission time, as well as optimizes the end system resource utilization. A burst is the basic data unit processed by the application. The data type of the burst is application dependent. For example, a burst for an image processing system corresponds to a photo. For video streaming system, a burst is the video chunk sent from the server to the client. In the burst forwarding network, the data source sends the entire burst using the line rate of the network interface card (NIC). The network forwards the burst with the same speed as it is injected into the network. In order to avoid any congestion, the network dynamically creates the end to end virtual channel [10] for each burst transmission. In the destination node, the bursts are received in sequence, the application can immediately process the data. This mechanism not only accelerates the burst data end to end transmission time, it also optimizes the computation resource utilization of the data processing.

This clause describes two use cases and highlights the current issues with them. These are (1). a metro gate control face recognition system, and (2). video surveillance system with real-time image processing. The simulation results given show the difference in performance between packet forwarding and burst forwarding. Finally, these applications are categorized into an application profile, aka the convergence of multiple sources with bounded network latency.

I.2.2 Use case description and generalization

a) Metro gate control face recognition system

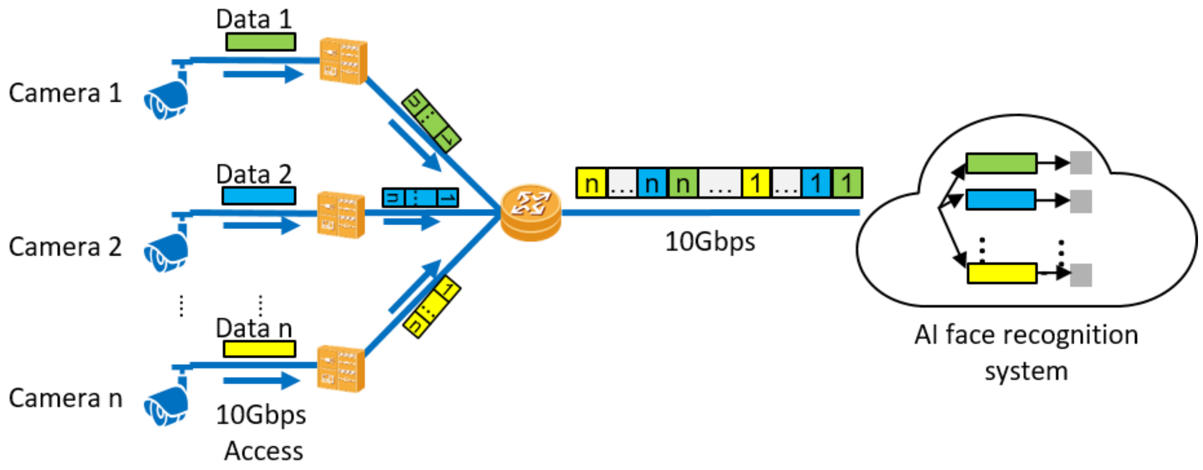


Figure 2 – Metro gate control face recognition system architecture

Figure 2 illustrates an example network architecture of the metro gate control face recognition system. In order to guarantee the high recognition accuracy, the metro gate camera takes a high-resolution picture for each passenger. The average photo size generated by the camera for one passenger is around 8MB. The cameras connect with the cloud AI system using 10Gbps leased lines. The timing details of the system are shown in the following table.

Table 2 – Latency requirement of the metro gate control face recognition system

Total Time	AI	Tx	Data Size	BW per gate	Access BW	No. of lines
200ms	7ms	193ms	8MB	332Mbps	10G	30

The average serve time for each passenger should be below 1.5 s, within which, 1.3 s are consumed by the door opening (0.3 s), the passenger passing through (0.7 s) and the door closing (0.3 s). The remaining 200 ms can be used by the end to end network communication and data processing. The AI cloud service consumes 7 ms to recognize a photo per network processor core. Therefore, the maximum end to end data transmission time is 193 ms. The physical bandwidth of the cloud access is 10 Gbit/s, which can support 30 concurrent photo transmissions.

Problem analysis:

The AI cloud service cannot process partially received photo data. It needs to wait until the full photo is received. As shown in Figure 3, if all cameras start sending photographs at the same time, ideally, the thirty (30) flows will be fully interleaved, packet by packet. Thirty concurrent photo transmissions take 193 ms to deliver an 8 MB photo over a 10 Gbit/s link. The AI cloud only has 7 ms to process thirty pictures. Therefore, the cloud service needs to reserve thirty NP cores for the upcoming data processing. However, during the data transmission period, no data are received in the AI cloud, and the NP cores are left idle. The efficiency of AI computation resource utilization is therefore only 3.5%.

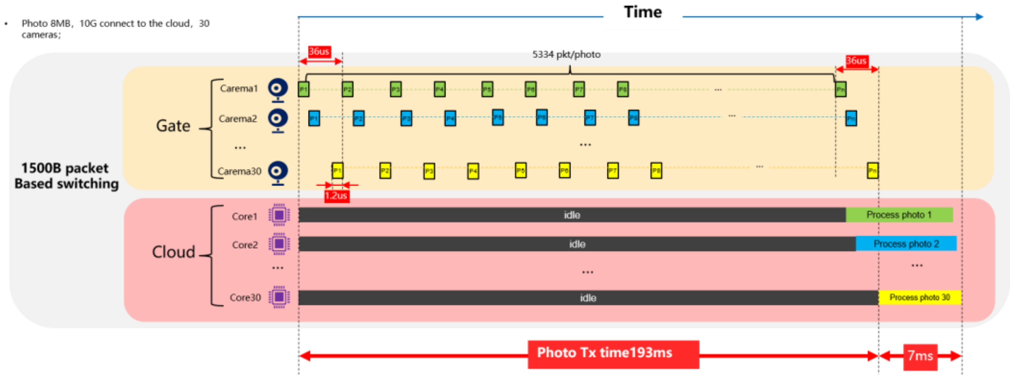


Figure 3 – Computation resource consumption of 30 concurrent photo transmissions

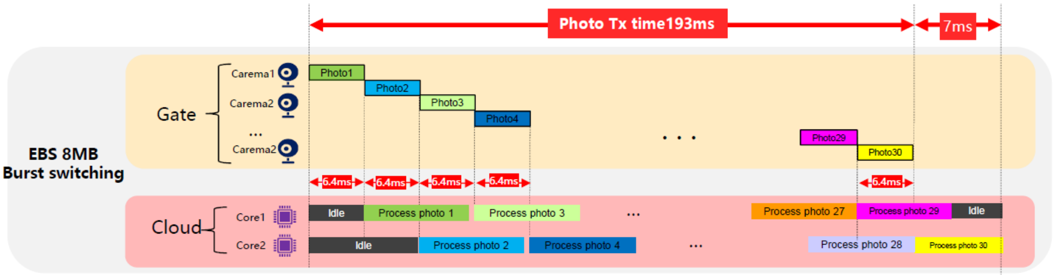


Figure 4 – Application-aware data forwarding

If the burst forwarding technology is utilized, the network forwards each photo one at a time. The photo is received by the AI cloud service much faster. As shown in Figure 4, every photo transmission occupies the entire bandwidth. For a 10 Gbps link, it only takes 6.4 ms to transmit one photo. Once the photo is received by the cloud AI, it can be immediately processed. Since each core takes 7 ms to process one photo, it requires maximally two NP cores to process the data. The computation resource utilization, in this case, is 54.6%.

The scenario described previously is the worst-case scenario and assumes that all the cameras send data at the same time. Simulations where the photo arrives in a poison distribution, is shown in Figure 5. This analysis shows that in the packet forwarding network, more than 60% of the traffic failed to meet the 200 ms deadline. The latest one was received at 260 ms. During this period, up-to 5 NP cores are needed to process the concurrently received photos.

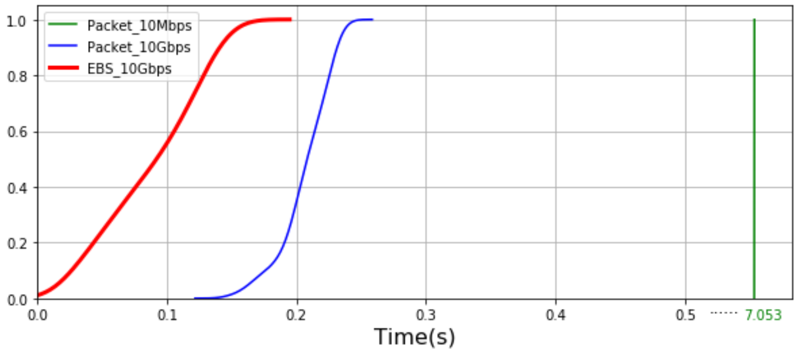


Figure 5 – CDF plot of the photo arrival time

b) Video surveillance system with real-time image processing

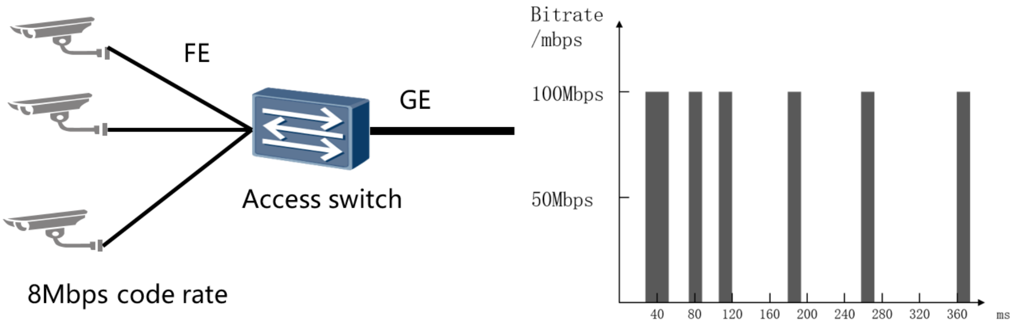


Figure 6 – Video surveillance system data uploading

The video surveillance system uploads the data collected from different cameras to the remote server. The received video streams are analysed in real-time in the remote server. The data generated from different cameras are required to be uploaded to the remote server within 1 s.

As shown in Figure 6, the camera accesses the network using an FE link. The average code rate for one camera is 8 Mbit/s. The egress port rate of the access switch is 1 Gbit/s. In theory, such a switch can support 125 camera connections. However, based on field test results, the switch only supports 30 cameras without losing any packets. The equivalent bandwidth consumption is only 24%.

Problem analysis:

As shown in Figure 7, the cameras access the network using an FE port. The GE egress port can only support ten (10) concurrent camera data transmissions. If there are more than 10 transmissions, the switch buffer starts to store the overloaded data. The access switch usually has a very shallow buffer. It is easy to lose packets due to buffer overflow. Although TCP will guarantee a reliable delivery, the retransmission mechanism consumes extra time and thus reduce the transmission speed.

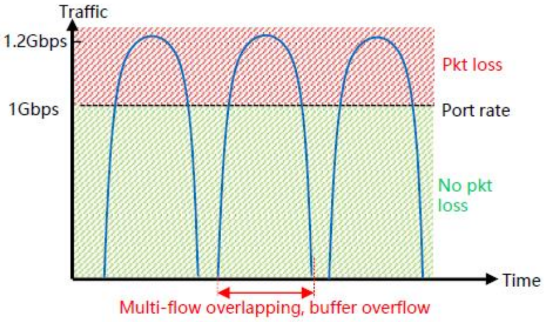


Figure 7 – Packet lose due to uncoordinated multi-flow overlapping

If the network forwards video chunks as the basic data unit, it is possible to limit the number of concurrent data transmission to never exceed 10. In this case, the accumulated ingress speed will never exceed the egress speed. No packet will be lost due to buffer overflow. Figure 8 shows the CDF of the data arrival rate with 110 camera connections. By using burst forwarding technology, all data can be delivered from the camera to the remote server within 1 second. However, when using TCP to transmit the same amount of data, more than 55% of the data fails to meet the deadline.

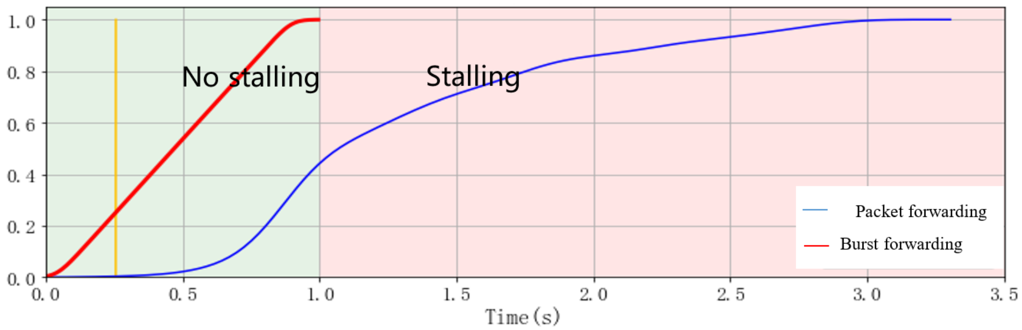


Figure 8 – CDF plot of video chunk uploading interval

c) Use case generalization

Burst forwarding technology can greatly reduce application data transmission time. Burst are transmitted sequentially in the network and received by the destination node with low latency. Mostly, applications that require quick feedback from received data benefit from burst forwarding technology. Based on the previous description, we further generalized these use cases into a category, aka, multi-source convergence with large data chunks under bounded latency. Such kind of applications usually share the following common characteristics.

- Application data are **originated from different data sources**. However, the generated data are centrally processed, e.g., in a remote cloud service.
- The network architecture of the application is usually an **aggregation tree** with converged bandwidth. The accumulated physical bandwidth of all the data sources is much higher than the access bandwidth to the cloud. However, the equivalent code rate matches the cloud access bandwidth. The data sources use high bandwidth to access the network, but only transmit data sporadically.
- The data transmission needs to be completed **within a bounded latency**. Overdue data are either too late to be useful or might break the pipeline of a closed loop control system.

I.2.3 Key network requirements

The network requirements, derived from comparing the differences between the burst forwarding network and the current packet-oriented network, are listed as follows:

- ***Bounded low latency***:

  The applications that can benefit most from ABF technology are those where multiple data sources need to converge to a central processing node with strictly bounded low latency, as elaborated in the above use case generalization.

- ***New forwarding manner***:

  The forwarding mechanism needs to change from packet forwarding network to a new technology such as burst forwarding network.

  Current IP networks forward data with packet granularity. However, the burst forwarding router continues transmitting a burst before switching to another one. An end to end virtual channel is created on demand for each burst transmission. If there are multiple virtual channels allocated to one physical port, the router should schedule each virtual channel using weighted round robin (WRR) [11]. The weight is proportional to the allocated bandwidth for the virtual channel.

  A burst forwarding router should identify the burst data boundary so that each burst can be transmitted consecutively. The network should support fast virtual channel establishment and tear down. Moreover, the burst forwarding network requires the flow control algorithm to ensure the network is congestion free. If more data needs to be sent at the same time than the network can handle, the extra burst transmission should be blocked and delayed until the previous burst transmission finishes.

- ***Burst sending in the data source***:

  Nowadays, almost all applications are developed on top of the socket interface directly or indirectly. By using the socket interface, applications can send data as a data stream (TCP) or datagram (UDP). Since the TCP interface provides reliable data transmission and self-adaptive throughput control, it is the primary choice for most applications. The flow management, security and congestion controls are developed in the user space, but nevertheless, current data forwarding mechanisms transmit data as a flow / stream. The throughput of each flow depends on the distributed congestion control algorithm.

  However, the burst forwarding network data source sends the burst using the NIC line rate. A new data forwarding mechanism is needed in the data source that supports large data sending without the limitations introduced by congestion control algorithms. Uncorrelated burst sending can cause incast problems. In order to eliminate network congestion, the data source should also cooperate with the flow control algorithm. During data transmission, the virtual channel needs to be created before forwarding the burst. If the virtual channel cannot be created due to bandwidth limitations, data transmission should be blocked and delayed. The data source should send back a pressure signal to the upper layer application to stop sending the data. Once the network becomes free, it should immediately forward the burst using line rate.

- ***Burst level grant send mechanism***:

  A bandwidth converged network usually has the in-cast problem. Nowadays, the network utilizes distributed congestion control algorithms to tackle this problem, e.g., CUBIC [13] and BBR [14]. Each data source keeps injecting data with its estimated network BDP. The throughput of the data source is greatly affected by other concurrent flows of data transmissions.

  The burst forwarding network requires the data source to send data using the line rate of the NIC. To avoid network congestion, each burst transmission needs to be carefully arranged. This mechanism is called the burst grant send mechanism. Different from congestion control algorithms which focus on transmission speed tuning, the grant send mechanism works as an on/off switch for the burst transmission. Once the burst transmission is granted, the burst is sent using line rate from the data source. If multiple data sources want to send data concurrently, the grant send mechanism needs to guarantee that the data injected into the network does not produce congestion that overflows the available router buffer. The burst forwarding network does not mandate any specific grant send algorithm. For the network with shallow router buffers, the buffer-free mechanisms, e.g., TDMA like or token-based algorithm can be used. Otherwise, a credit-based flow control [15] mechanism could be used with manageable buffer consumption.

I.2.4 Evaluation of the abstracted requirement dimensions

The scores below are given by the contributor based on the analysis of network requirements of the use case.

Bandwidth: 8; Time: 5; Security: 2; Artificial Intelligence (AI): 2; ManyNets: 2

(Note that all the scores are given according to the relative importance of a specific network requirement: 1 to 3 are for relatively LOW requirement; 4 to 6 are for MEDIUM requirement; 7 to 9 are for relatively HIGH requirement; and 10 means EXTREMELY demanding requirement)

I.3 Emergency and disaster rescue (EDR)

I.3.1 Background and introduction

The global scale of tragic events such as the coronavirus pandemic (COVID-19) clearly demonstrates the need for reliable, robust and fit for purpose digital infrastructure and the great importance and relevance for the future of humanity of the work carried out in the FG NET-2030, including the concepts and system developed at NIIR "Mass service of individualized control for the population rescue (MSIC) in the event of all kinds of emergency situation anywhere in the place and at any time" (4th ITU Workshop on Network 2030, Saint-Petersburg, Russia Federation, May 21-23, 2019).

In order to minimize human losses, in the case of only one of the types of possible natural and man-made emergencies, for example the current COVID-19 situation, it is necessary to ensure individualized management and control of the safe behaviour of everyone without exception in a relatively short period of time between the onset of the emergency and the onset of its catastrophic phase in people. Mankind has had to invent separate solutions on the go. However, since all kinds of emergencies can happen simultaneously, the consequences of, for example, an earthquake in a modern metropolis, which may be accompanied by other types of emergencies are beyond severe. The invention therefore of separate solutions on the go requires multiple increase in ICT capabilities that can only be realized by Network 2030. All the following examples of the use cases of "Mass service of individualized control for the population rescue (MSIC) in the event of all kinds of emergency situation anywhere in the place and at any time" on a large scale can only be implemented with the implementation of the FG NET-2030 deliverables.

I.3.2 Use case description

Full implementation of the EDR service is possible only with the implementation of all development plans outlined in FG NET-2030. Of particular importance in the proposed service is that:

- it will be available to any subscriber "anywhere, anytime and for everyone" in the event of any type of emergency of technogenic and natural origin, that is,

$$EDR = f\ (ESi,\ ...\ n)$$

where n is the finite number of possible, even with a small probability, types of emergencies;

- it provides an individualized qualified (expert, most optimal in the current situation) self-evacuation control in the nearest safe area (see Figure 9) for this type of ESi.

Figure 9 shows a block diagram of the formation of EDR = f (ESi, ... n) – mass individualized services for control subscriber self-evacuation. Localization (decentralization) of control (Figure 12) is very important when organizing such a service.

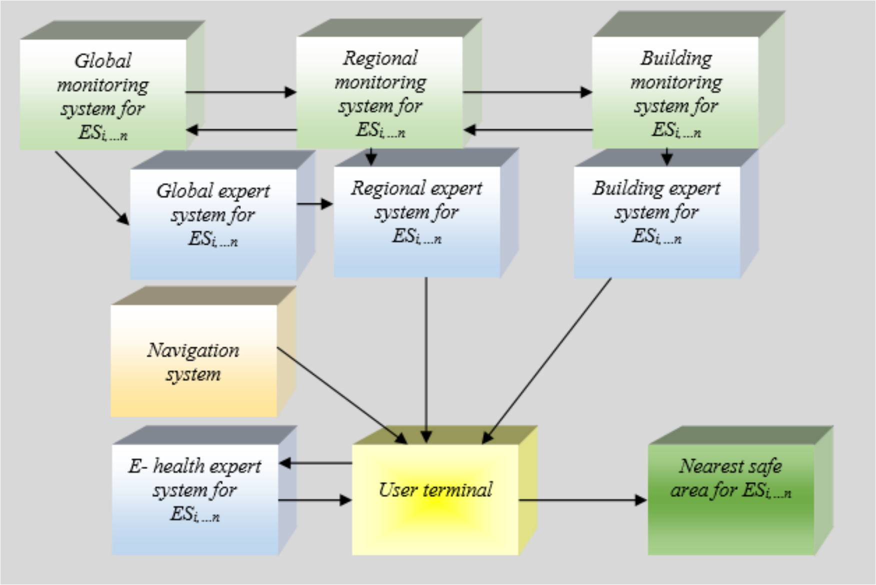

Global monitoring system for $ES_{i,...n}$
Regional monitoring system for $ES_{i,...n}$
Building monitoring system for $ES_{i,...n}$
Global expert system for $ES_{i,...n}$
Regional expert system for $ES_{i,...n}$
Building expert system for $ES_{i,...n}$
Navigation system
E- health expert system for $ES_{i,...n}$
User terminal
Nearest safe area for $ES_{i,...n}$

Figure 9 – EDR system block diagram

Of course, the subscriber's behaviour is important, since this reduces network delays, which is of particular importance in the conditions of a short time between the beginning of To and Tk.

Subscriber terminal interactions with expert systems: the following are examples of the organization of object expert systems (case 1 and case 2. Figure 10 and Figure 1 of [21]), global, regional and local monitoring systems for emergencies of natural origin (Figure 11), configuration of the building expert system (Figure 12) as part of a RDR = f (Esi,…,n) system block diagram as shown in Figure 9.

The massive services for Emergency and Disaster Rescue (EDR) are known as enabling instantaneous notice to human and valuable objects (e.g., humanoid robots) with guided information on self-saving or self-evacuation by using ubiquitously collected sensing data at global scale.

The fundamental difference between two Emergency Situations (ES), i.e., natural and technogenic origin, is precisely in the moment of the beginning of the ES. Therefore, two cases are elaborated in detail as follows, for two different catastrophic phases given by **T*k***.

Case I: T*k* > 10 minutes

The difference lies in the fact that in the case when **T*k*** > 10 minutes, it is possible, with the help of an organized interaction of the subscriber terminal and sensors based on the vastly deployed IoT, to organize an individualized control of the rescue of people from a specific location (e.g., school building, music auditorium, etc.), inside which or nearby, an ES occurred. Thus, the system will facilitate the self-evacuation from the facility to a safe place, notifying people who are in it, including non-residents and people with disabilities, before **T*k*** comes. The detailed solutions have been described in [16][17].

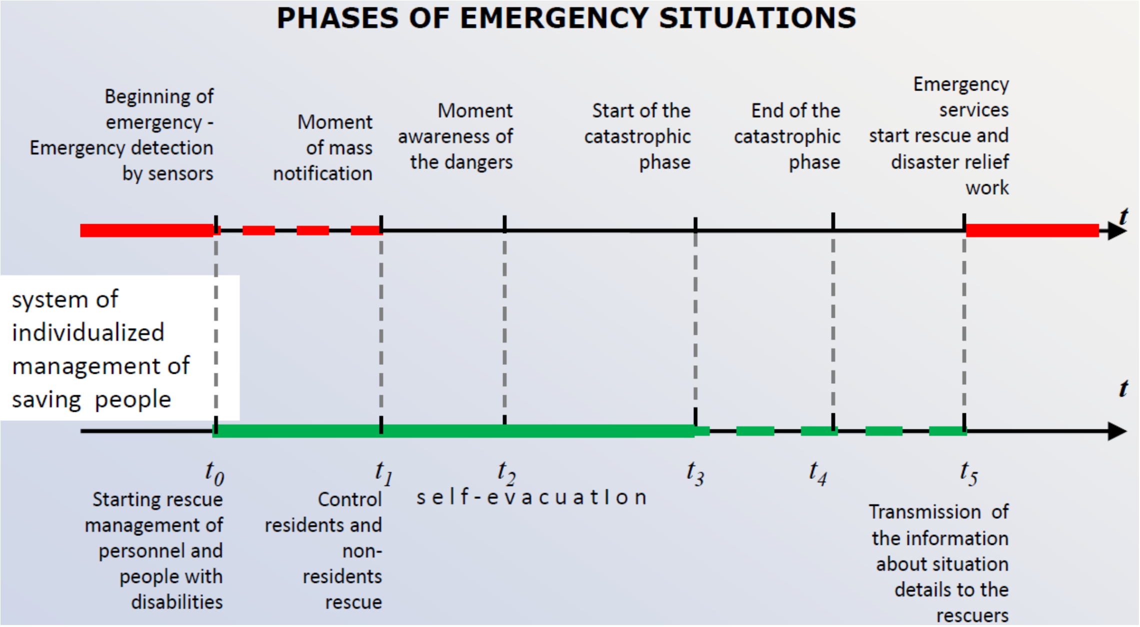

PHASES OF EMERGENCY SITUATIONS
Beginning of emergency - Emergency detection by sensors
Moment of mass notification
Moment awareness of the dangers
Start of the catastrophic phase
End of the catastrophic phase
Emergency services start rescue and disaster relief work
t
system of individualized management of saving people
t
t_0
t_1
t_2
t_3
t_4
t_5
Starting rescue management of personnel and people with disabilities
Control residents and non-residents rescue
self-evacuation
Transmission of the information about situation details to the rescuers

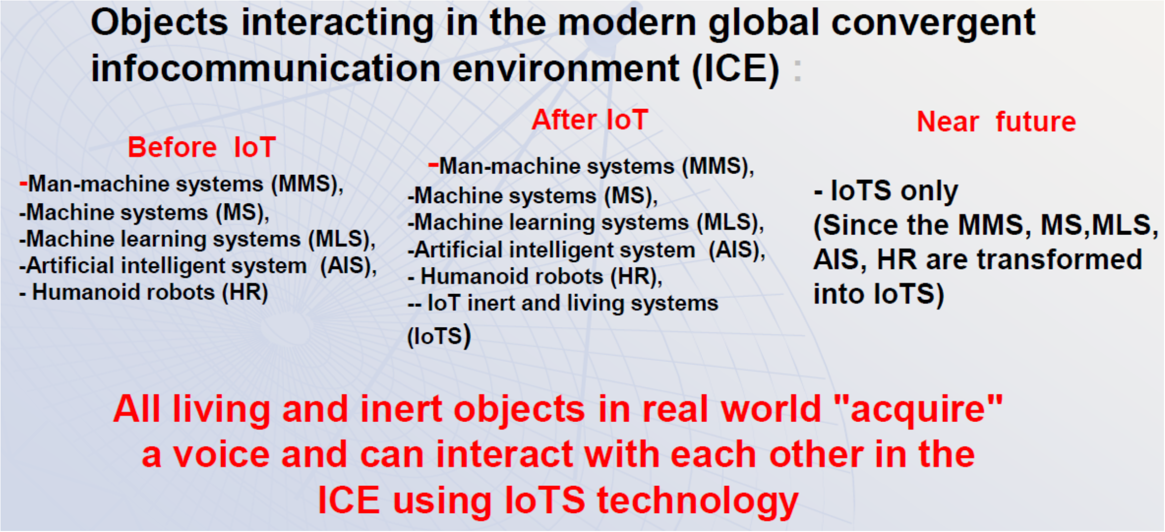
Figure 10 – The effect achieved by using the received warning signals received by the subscriber terminal from the IoT environmental sensors and ES models

Case II: T*k* = 0

For the ES when **T*k*** = 0, e.g., an earthquake or explosion, the solutions described above are not suitable. As a result, it is necessary to have warning signals at least 10 minutes before ES. Under such condition, it is then possible to organize the individualized control of the self-evacuation to a safe place as described in the previous section. Via adopting massive IoT, it turns out that sensors have increased sensitivity to warning signals of such ES, which are targeting living (including human) and inert objects of nature. Potential solutions are described in Recommendation ITU-T Y.4121 [21].

In a typical site of the proposed hybrid monitoring system, signals received from natural IoT objects are processed in conjunction with signals from existing sensors on traditional monitoring networks. Such joint processing of the readings from sensors of different physical nature makes it possible to detect even very weak warning signals, for instance, earthquakes.

The above two cases under different conditions are necessary to solve the issues of large-scale implementation of massive services for EDR, with the help of IoT to create a hyper-connected world. Thus, the following figure shows the vision of EDR relevant process.



Objects interacting in the modern global convergent infocommunication environment (ICE) :

Before IoT

-Man-machine systems (MMS),
-Machine systems (MS),
-Machine learning systems (MLS),
-Artificial intelligent system (AIS),
- Humanoid robots (HR)

After IoT

-Man-machine systems (MMS),
-Machine systems (MS),
-Machine learning systems (MLS),
-Artificial intelligent system (AIS),
- Humanoid robots (HR),
-- IoT inert and living systems (IoTS)

Near future

- IoTS only
(Since the MMS, MS,MLS, AIS, HR are transformed into IoTS)

All living and inert objects in real world "acquire" a voice and can interact with each other in the ICE using IoTS technology

Figure 11 – The potential of IoT to formation of a hyper-connected world and vision of EDR process

In addition, such mass services as a whole cannot be created without global cooperation with individualized vast deployments across all countries. These developments backed by novel research will make a qualitative leap in implementing plans for creating services for the entire human population, so that these services can be called "anywhere in the world and at any time".

I.3.3 Key network requirements

Below are some preliminary remarks.

1) When determining the requirements for networks that can implement EDR, it is necessary to consider that EDR is a mass service and should be available to any user anywhere, anytime. Such networks can only be public communication networks (PCN). For this reason, it is very important to identify in future promising networks the place (requirements) of PCN provided for in the considerations of FG NET-2030. The capabilities of PCN to provide synchronization are also very important, since the control is carried out for different subscribers who are nearby at the time of the emergency.

2) EDR must be considered on two scales: 1) at the object scale, 2) at the regional and global scales (Figure 9). In these two cases, the requirements in the frequency and speed bands, although equally high, are different in execution. So, for the object system, high requirements for PCN can be achieved today even on 4G networks, since acceptable EDR requirements can be implemented using SCN. Thus, the implementation of EDR services is possible today, but only on an object scale, and in order to make this service available on a regional and especially global scale, that is, to implement "anywhere, anytime and for everyone", it is necessary to realize all capabilities that FG NET-2030 has outlined until 2030 and beyond.

3) It is very important to focus on the features of the functioning of EDR. The network supporting the operation of EDR operates in two modes: a) transmission of control signals: the network operates both for Case 1 (Tk> T0) and for Case 2 (Tk = T0) only in a short time of emergency (the transmission schedule for this traffic is presented on Figure 10), in this mode the traffic volume is small, since only control information is transmitted, priority is required for these signals at any time, since emergencies can occur at anytime and anywhere; b) traffic is transmitted to update global, regional and object expert systems (Figure 9) with new data: in this case the traffic volume can be large, but it is formed and transmitted as necessary, in this case there is no need for priority mode.

Also, it should be noted that there are two types of messages: a) Vc – control information, well-structured, small amount and b) Ve – information from expert object, regional and global expert to update the subscriber's integrated expert system for emergency preparedness.

The key challenges of EDR cases do not follow the traditional network metrics such as bandwidth, latency, reliability, and so forth, since EDR mainly depends on worldwide deployment of intelligent sensing devices. Thus, the key requirements also fall into some non-technical aspects:

– ***Deployment maturity***: It is needed to promote fast deployment for all the countries in the world in every single country to have intelligent sensors equipped around human communities and valuable assets. It is assumed that this deployment process has already been completed for significant objects (at the object scale), but such a deployment process is envisioned to take a long time for full development, in the next decade, or even longer. For instance, one practical vision towards deploying trillions of IoT devices is foreseen [18]: all the data collected from the huge IoT sensors must be quickly processed and comparable to useful information and actions that can improve EDR service.

– ***Data Intelligence***: All the data collected from vast IoT sensors should be promptly handled and mapped to guide useful actions that can enable EDR services in a better way.

– ***High-precision response with critical network infrastructure***: Once warning notices are required to be broadcasted to destination EDR areas, these notices should be forwarded to individual objects (i.e., living or non-living) with high precision (e.g., tolerable latency to exact objects and all stakeholders) over critical network infrastructure which should always be set aside, or at least quickly restored in the EDR conditions.

– ***Small and bounded jitter***: In order to provide time deterministic services, such as remote surgery and remote-control systems, it is required a small and bounded jitter (sub microsecond level).

To develop key implementation requirements, examples of technical solutions that will be used are set out in some ITU-T Recommendations [20][21][22][23].

In particular, it is required:

1) The effectiveness of individualized management of rescue of people in case of emergencies is ensured by the construction of a stable info-communication system, which should include several means of communication, which together make it possible to realize the system's resistance to the main types of vulnerabilities.

2) One of the most significant types of vulnerabilities in the public telecommunication networks is their sensitivity to mass calls (overloads), which limits their applicability for information transfer in order to manage the rescue of people in case of emergencies.

3) The increase in traffic intensity in the public telecommunication networks in the emergency zone can exceed the average traffic value by 3–6 times, which leads to an increase in the probability of loss of calls to 90% or more.

4) The traffic intensity in the public telecommunication networks depends on the awareness of the subscribers, determined by the time of delivery of data or control commands.

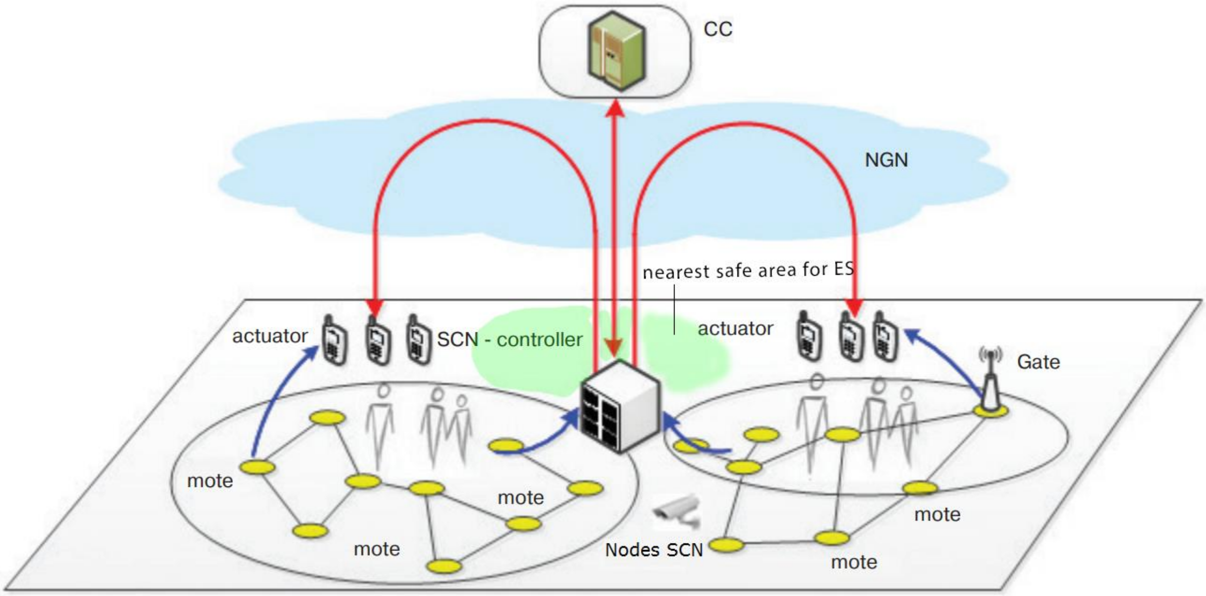


Figure 12 – Communications complex in the emergency zone using SCS

5) The use of SCN allows increasing the stability of the info-communication system to various vulnerabilities, including those caused by public communication network (PCN) overloads by timely informing subscribers in the emergency zone.

6) The task of constructing SCN can be solved by the methods of constructing wireless sensor networks as the task of optimizing the quality of traffic service taking into account the structural parameters of the network, the requirements for the lifetime and the set of services provided.

EDR (Figure 9) should be able to manage the subscriber's self-evacuation from any point in space on planet Earth, including when several emergencies occur at once. Figure 9 shows a block diagram of the formation at the subscriber terminal of the subscriber, and corresponding expert system, which, when an emergency occurs, begins to control his self-evacuation.

The growth of wireless communications and networks all over the world has put unprecedented demand on the need for spectrum and its use. The projected demand for wireless systems in the FG NET-2030 project with ubiquitous connectivity, high speed and low latency highlighted the problems of RF spectrum deficiency and interference management. In addition, upcoming commercial deployments should work in harmony with scientific and passive applications such as radio astronomy, atmospheric science, and weather forecasting. The key to an interconnected future is to establish harmony between the scientific use of the electromagnetic spectrum with technological advances in the field of high-speed data transmission with low latency, secure communication between conventional devices, autonomous vehicles and many other platforms, as well as scientific research and practical development of the causes of various kind of emergency. This research and development will form object, regional and global monitoring systems for various types of emergency situations and the corresponding expert systems. Moreover, this number is infinite, and even the most unlikely emergencies can be included here. Having analyzed almost all the technical solutions and services proposed in this report that are recommended for implementation by 2030 and beyond, it can be stated that most of them can be part of expert systems of three service levels.

At present, only system options for the object system have been implemented. So that all the requirements for 4G and 5G networks correspond. The transition to "anywhere, anytime and for everyone" is possible only if all the technical solutions planned are implemented. The higher the performance of communication networks, the greater the percentage of saved people.

NOTE – In addition to the above, other network requirements for this use case concern bandwidth, latency, synchronization, reliability, protocol requirements, functional requirements and architectural requirements, but are not discussed in this report.

I.3.4 The Evaluation of the Abstracted Requirement Dimensions

The scores below are given by the contributor based on the analysis of network requirements of the use case.

Bandwidth: 5; Time: 6; Security: 9; Artificial Intelligence (AI): 8; ManyNets: 5

(Note that all the scores are given according to the relative importance of a specific network requirement: 1 to 3 are for relatively LOW requirement; 4 to 6 are for MEDIUM requirement; 7 to 9 are for relatively HIGH requirement; and 10 means EXTREMELY demanding requirement)

I.4 Socialized Internet of Things (SIoT)

I.4.1 Use case description

The number of objects that are reachable over the Internet is now close to 10 billion and this number is increasing rapidly [24]. These devices produce a vast amount of data and provide a remarkable number of services which need to be meshed and interconnected to extract the real value for the benefit of the society. This can be achieved through centralized approaches, where objects belonging to each platform are connected and managed by a centralized component that takes care of blending the data coming from different objects to extract the useful information. Different platforms can then be interconnected to avoid the formation of the often-criticized *silo effect* of the Intranets of Things. The control of interactions and information flows will be in the hands of the central components of each platform, which will decide what can get out of each realm and how it can be shared with the external world.

In contrast to this approach, the *Social Internet of Things* (SIoT) model intends to exploit the potential of social networking technologies to develop a decentralized approach to foster the interactions among objects that belong to communities of trillions of members. The use of social network technologies presents a different vision where objects are capable of creating and managing social-like relationships with each other in an (almost) autonomous way [25][26]. In general, advantages of the SIoT are:

– by appropriately setting the rules applied to establish social relationships between objects, the resulting social graph has desirable structural characteristics, i.e., its diameter is small, and it is navigable;

– it enables new communication primitives, like *Sociocast*, which goes well beyond traditional unicast/multicast/broadcast and identifies the destinations of a given message based on their position in the social graph [27][28];

– it simplifies the establishment of trustworthy relationships between objects so enabling differentiated level of security and therefore, reducing its burden;

– it enables resource/service discovery across different IoT platforms.

These advantages have been demonstrated in real-world deployments for several application fields, such as transportation, energy management and eHealth.

To implement this scenario, the network operator should take the pivotal role to support the creation and management of the social links among the objects by providing the appropriate services to augment the connected objects with the social capabilities. Accordingly, each object is supported by the network that provides the functionalities and APIs to implement a virtualized social counterpart (i.e., the virtual entity) for an object to opportunistically interact with the other virtual entities in the network.

A real scenario is one related to the delivery of parcels, where the explosion of e-commerce characterized by exponentially increasing volumes of orders has radically changed the way in which goods are delivered to customers, especially in the last mile. Such trends are expected to continue, with the recent COVID-19 pandemic giving a further boost which will not disappear at the end of the crisis. This opens an opportunity for traditional logistics operators to define new services and access untapped markets. It is however clear that to seize such opportunities logistic operators need to address new challenges. Customers are becoming more demanding, in terms of pushing for new service models such as *same-day delivery*. Furthermore, several municipalities are closing cities to vehicle traffic, reducing the time window available for deliveries and pickups significantly. Finally, new players are entering the logistics industry and applying completely new business models, like logistics-as-a-service or on-demand logistics, thus radically changing the competitive landscape.

In such a context, it is mandatory for logistics operators to put solutions into place which minimize costs and maximize sustainability.

To achieve such objectives, it is fundamental to continuously monitor the state of all logistics assets, collect large amounts of data from the environment and process such data for optimization purposes, by exploiting the possibilities offered by multimodality and cooperation between non-competing players. Also, there are several pilots aimed at demonstrating the effectiveness of using unmanned (both aerial and terrestrial) vehicles both for pickups and deliveries.

According to a recent study Internet of Things (IoT) technologies will play a key role in such context [19].

A recent approach proposed in this domain is to exploit the cited Social Internet of Things (SIoT) paradigm (see http://www.cog-lo.eu).

In the context of logistics, specific advantages brought by the SIoT are:

– Logistic operations require the processing of large amounts of data generated by heterogeneous sources belonging to different organizations. The use of Sociocast helps defining the scope of each information item.

– Relationships established by social logistic objects can build links between IoT platforms belonging to different stakeholders so enabling more efficient transport and logistics services.

In Figure 13, we sketch the assets of several logistic operators (identified with different colours: blue, green, black, yellow) operating in a certain area. Each of the assets is represented by a social virtual object which is a node of the SIoT graph as depicted in Figure 13. Observe that assets that belong to the same logistic operators and/or are nearby are linked in the SIoT graph. Also, vehicles 1 and 13 have a relationship because they are expected to deliver parcels nearby.

In the following we will provide a simple example in which the SIoT approach supports collaborative logistics.

Consider the case in which a vehicle fails while delivering. All parcels transported by this vehicle must be re-loaded onto other vehicles for their delivery. This will require a re-routing of other vehicles. Note that collaboration with other logistic providers is likely to be needed in such a context.

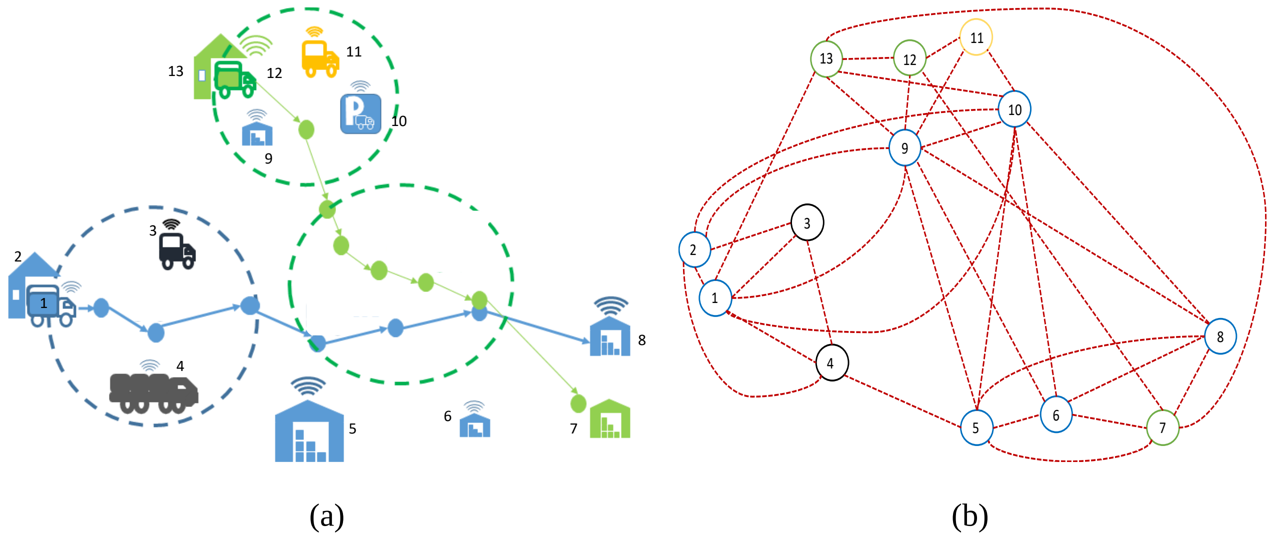


Figure 13 – (a) SIoT enabled logistic scenario (b) SIoT graph of the logistics scenario

Therefore, the SIoT paradigm can be exploited as follows.

Each parcel in the failed vehicle will notify the vehicles (those in the list of its "friends", and plan to pass nearby its destination and have sufficient space/capacity) that it needs a new pickup. Note that such vehicles can belong to logistic operators other than the one of the failed vehicle. The SIoT in fact creates relationships between objects (and thus parcels and vehicles) that are close to each other. Note that configuration policies can be defined by the owner of each logistic operators about the disclosure of information about its own fleet. In this way the SIoT guarantees trustworthiness. The driver of the vehicle receiving the notification will decide whether to pick the parcel up or not.

Also, it might be that it is convenient to use UAVs (Unmanned aerial vehicle) to transfer parcels from the failed vehicle to the new ones. In this case, if there are strong trust relationships between the major actors, it is possible to temporarily transfer the control of the UAV from one operator to the other. In this case the advantages of exploiting a network of relationships based on trust can be extremely beneficial.

I.4.2 Key network requirements

The requirements set by the SIoT on the network are:

- ***Open network service interfaces***: This will enable new networking primitives such as Sociocast [24][25]. To this purpose, SDN/NFV techniques might be exploited.
- ***Support for friendships creation***: Social relationships among devices need to be established by monitoring device positions and the contacts among devices, e.g., through short-range connectivity or by analysing the data exchanged among them over the network. Proper APIs are required responsible for such operations and operating in a transparent manner for the end-user, by allowing the user to keep control of the data.
- ***Virtualization of the social objects***: The network should provide the APIs to instantiate social virtual objects associated to the objects connected to the network.
- ***Security/privacy tools and infrastructure***: While the SIoT fully takes the responsibility of managing trust between smart objects, we observe that the network should provide tools to protect the SIoT from attacks. In fact, the SIoT elements contain data that can be exploited to achieve sensible information about the users.
- ***Availability of computing and storage resources at the edge of the network***: In the SIoT each object is represented by a virtual entity instantiated in a nearby server. Such servers

must be "inside" the network to guarantee significant availability of bandwidth supporting the many interactions needed for SIoT relationship management. However, it should also be close to the physical object to reduce delay. It follows that effective SIoT deployment requires a dense infrastructure of computing and storage elements at the edge of the network.

– ***Mobility***: Some intelligent things (e.g., smart meter, environmental sensors) are static, whilst others (e.g., cars, public transport means, smartphones) have high mobility or group mobility. Thus, the network needs to flexibly support mobility on-demand and track objects to update social relationships accordingly and to effectively perform location discovery of moving SIoT objects.

– ***Energy efficiency***: Most "things" are battery operated and therefore the network should put in place techniques aimed at the minimizing the number of operations an object is required to execute.

– ***Latency***: Low latency is required to enable the control of UAV's exploited for the delivery of parcels.

I.4.3 The Evaluation of the Abstracted Requirement Dimensions

The scores below are given by the contributor based on the analysis of network requirements of the use case.

Bandwidth: 7; Time: 9; Security: 9; Artificial Intelligence (AI): 7; ManyNets: 8

(Note that all the scores are given according to the relative importance of a specific network requirement: 1 to 3 are for relatively LOW requirement; 4 to 6 are for MEDIUM requirement; 7 to 9 are for relatively HIGH requirement; and 10 means EXTREMELY demanding requirement)

I.5 Connectivity and sharing of pervasively distributed AI data, models and knowledge (CSAI)

I.5.1 Use case description

This use case describes a future network scenario which outlines the radical shift of the Internet of Things (IoT) paradigm from *connected things* to *connected intelligent things*.

In this use case, IoT devices are evolutions of dummy sensors and actuators into more sophisticated, intelligent objects that can assist the user and take decisions either autonomously or interactively with humans and/or other devices thanks to artificial intelligence (AI) based algorithms.

Currently, the most common use cases where AI is associated to IoT systems, are those aimed at predicting future insights, detecting anomalies and taking control decisions starting from IoT streamed data. In the e-health domain, mobile personal assistants continuously monitor health data via bio sensors, and can predict critical situations like low blood sugar level and trigger alerts accordingly. Autonomous cars can feed image recognition algorithms with data provided by a multitude of on-board sensors to promptly detect obstacles and manoeuvre accordingly. In smart cities, a camera streams its data to face recognition algorithms for surveillance purposes. Predictive maintenance and condition monitoring can be performed starting from data collected from sensors embedded in a production line.

Typically, solutions for such reference applications leverage a *centralized paradigm* (commonly implemented in the remote cloud). AI algorithms (e.g., deep learning (DL)) are memory- and power-hungry. Hence, most off-the-shelf IoT devices just send input raw data to the cloud which is then in charge of the model building/training as well as of the inference, whose results need to be sent back to requesting devices.

The edge will soon complement the cloud in enabling the deployment of intelligent services. Indeed, edge AI is mentioned among the top emerging technologies by Gartner in 2019 [29]. A recent IDC report [30] estimates that 45% of IoT-generated data will be stored, processed and analysed close or at the edge of the network by 2025, with increasing market opportunity for AI-optimized processors. If DL services are deployed close to the requesting users, the latency and cost of sending data to the cloud for processing will be reduced, with benefits in terms of privacy preservation and offloading of the core network infrastructure.

However, a true revolution will be achieved when AI extends along the cloud-to-things continuum, embedded in IoT devices, implemented at the network edge and in the remote cloud. This would be possible thanks to recent improvements in purpose-built AI-optimized processors and achieved advancements related to the possibility to embed AI inference in general-purpose processors. Figure 1 provides a high-level illustration of the use case dealing with the connectivity and sharing of pervasively distributed AI data, models and knowledge.

Such a futuristic scenario raises several daunting challenges for the design of Network 2030.

The pervasive distribution of AI capabilities to end-devices, network nodes, edge/cloud facilities is not like the placement of generic computing tasks and their subsequent connectivity and chaining. It goes well beyond since a proper understanding of AI peculiarities is required when designing networking procedures that enable a scenario where AI workloads and AI data is dynamically spread over a pervasive AI deployment, to properly match application requirements, especially in terms of accuracy and privacy.

A native AI-awareness is essential in all network operations. For instance, part of the DL inference can be performed in IoT devices and heavier (training) tasks offloaded to edge and cloud facilities. As a result, according to the specific AI deployment, data of variable size (i.e., bulky raw data, intermediate data, AI models, updated model parameters, inference results) and in different formats coming from massively deployed intelligent things need to be efficiently exchanged in the network, meeting latency demands whenever real time decisions need to be taken. Multiple AI components provided by IoT devices can be pooled together for more accurate inference results. For instance, layers of the same neural network can be split over multiple devices, according to their capabilities. The pooling procedures will benefit from decentralized networking approaches where devices have to collaborate and have capabilities to share AI-related resources and data according to the needs of the environment and applications. For instance, a newly installed surveillance camera in an office building can ask a camera deployed in a different building of the same company to share the updated objects detection and tracking models, with no need to train the model from scratch.

The network has to offer the possibility of facilitating such pervasive AI deployment among intelligent things which may also need to interact autonomously. Hence, reachability of AI components needs to be ensured for the composition of an AI pipeline. More flexible network addressing schemes are required to properly name the AI components regardless of the specific position in the network where they are placed. Discovery procedures are also required to identify the most suitable things to contribute to AI-based services. Device-to-device connectivity would be required to set-up autonomously and in a resilient manner, whenever privacy-sensitive data needs to be exchanged. Once properly named AI components are discovered, the network will be in charge of properly routing requests towards them. Conventional IP-based addressing and flow-based routing do not match the envisioned scenario.

For instance, groups of pervasively distributed AI components can either be simultaneously queried to perform some training tasks starting from their disjointed data subsets (e.g., in the case of federated learning) or be the simultaneous recipients of updated models. Existing network primitives cannot address such demands and novel ones (e.g., group-based push/pull) are entailed to this purpose.

Moreover, AI inference results, once computed, could be reused and serve different requests. To this aim, caching procedures could be highly relevant. Such procedures should be designed directly at the network layer to be faster and more flexibly implemented.

Nonetheless such a capillary AI deployment, more synergistically connecting the AI and IoT realms, places even more demanding requirements upon the design of future networks, entailing novel communication schemes, proper addressing solutions and the support of strict KPIs.

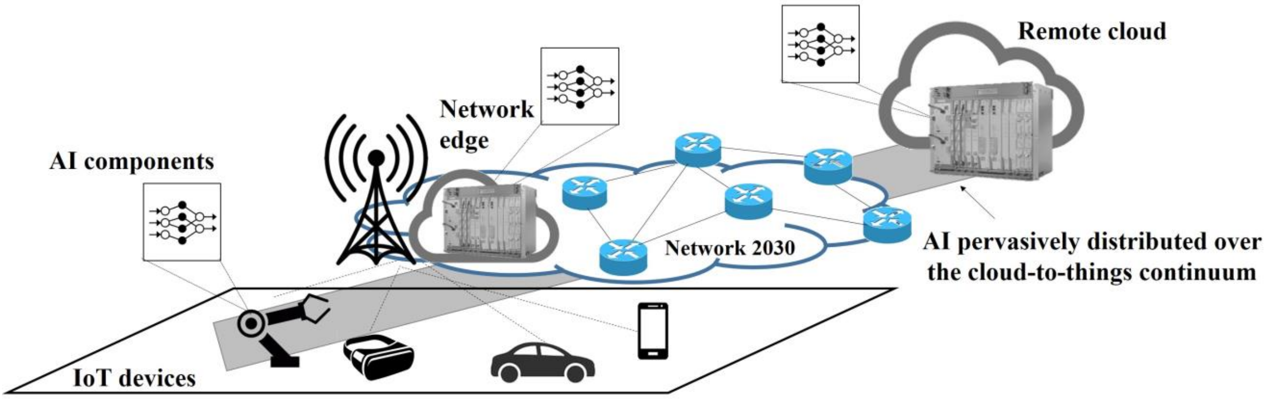

Remote cloud
Network edge
AI components
Network 2030
AI pervasively distributed over the cloud-to-things continuum
IoT devices

Figure 14 – Example reference architecture for CSAI

I.5.2 Key network requirements

– ***Mobility***: Intelligent things maybe either mobile (e.g., cars, smartphones carried by users) or static (e.g., smart meters, cameras). Thus, the network needs to flexibly support mobility on-demand.

– ***Energy efficiency***: The decision about where to place AI components and how to interconnect them should be taken by accounting for the possible involvement of battery-constrained intelligent devices. Networking protocols are needed to ensure low energy consumption in the interactions among intelligent things to share either raw data or inferred knowledge.

– ***Virtualization***: AI solutions would largely benefit from virtualization techniques able to deploy components in an agile manner. They can be packaged inside containers [31] (and even into more lightweight platforms) while reducing the deployment footprint in terms of processing and memory, to better match resource constraints of edge/IoT devices.

– ***Joint network, intelligence and computing orchestration***: The decision about how to distribute AI workloads should be performed through a synergic integration of computing, caching and communication (3C) resources [32], to account for computing resource availability, network conditions and popularity of requests for caching of models/inference. Moreover, it should go well beyond existing joint 3C solutions and specifically account for peculiar DL models requirements, e.g., privacy and accuracy. Such *AI-awareness should be built by design* in orchestration mechanisms.

– ***Bandwidth and capacity***: Massively deployed intelligent things may generate extremely large amounts of data to enable the adequate training of AI models [33]. According to the deployed AI pipeline, either large amounts of raw datasets/intermediate results to be trained, or trained/updated models need to be exchanged among several entities (i.e., IoT devices, edge nodes, cloud facilities), hence, large bandwidth and capacity may be required.

– ***Latency***: Data exchange among entities needs to be as fast as possible, in the order of < 1ms in the case of real-time decision making (e.g., in an industrial plant, for an autonomous car, or for remote surgery), hence requiring extremely low-latency data transmission over both the radio interface and the core network segment.

– ***AI-aware addressing***: In a pervasive AI deployment, every entity can contribute to the AI workflow. Flexible addressing capability is, thus, needed to optimally address AI components (e.g., DL models) associated to intelligent objects to facilitate discovery and composition procedures.

– ***Uniform exposure***: Many purpose-built and fragmented AI solutions will be developed to serve a specific use case through proprietary APIs. To make them interoperable and flexibly chained, the network should provide uniform exposure interfaces to describe AI capabilities of intelligent things to third parties and ensure reusability.

– ***Network programmability***: AI components spread along the cloud-to-things continuum should be chained to ensure the exchange of data of variable sizes with low-latency and high-bandwidth demands in a flexible and dynamic manner. Moreover, it could be common that AI models (and updated ones in case of incremental deployment) need to be simultaneously spread to multiple devices (e.g., updated object/face detection models for cameras sharing the surveillance task in a smart city, or, language recognition app updates for smartphones of the same brand). Hence, proper network primitives, besides multicast and broadcast, may be required which recognize the entities to be reached and efficiently forward data to them accordingly.

– ***Security and privacy***: Since most of the information used to build inference models are associated to personal devices and the way users exploit and carry them (e.g., smartphones, cars, wearables), adequate security and privacy frameworks should be conceived.

I.5.3 Evaluation of the abstracted requirement dimensions

The scores below are given by the contributor based on the analysis of network requirements of the use case.

Bandwidth: 8; Time: 9; Security: 8; Artificial Intelligence (AI): 8; ManyNets: 8

(Note that all the scores are given according to the relative importance of a specific network requirement: 1 to 3 are for relatively LOW requirement; 4 to 6 are for MEDIUM requirement; 7 to 9 are for relatively HIGH requirement; and 10 means EXTREMELY demanding requirement)

Part II: Use case requirement scoring and analysis

II.1 Graphic representations of the network requirements

The five representative use cases described in this report have been further evaluated according to five abstract network requirement dimensions, as widely discussed in [34]. These are namely: **Bandwidth**, **Time**, **Security**, **Artificial Intelligence (AI)**, and **ManyNets**. The relative scores for these 5 dimensions, ranging from 1 to 10, as identified in part I, are shown in Figures 15 and 16 using two different graphical representations.

It is important to note that the five dimensions identified in this report have been abstracted from a relevant set of network requirements considered within Sub-Group 1 of FG NET-2030, as shown in Table 3 below.

Table 3 – Abstract dimensions with relevant network requirements

Abstracted dimensions	Relevant network requirements [based on the requirements identified in Part I of this report]
Bandwidth	Bandwidth; QoS; flexibility; and adaptable transport
Time	Latency; synchronisation; jitter; accuracy; scheduling; and geolocation accuracy
Security	Security; privacy; reliability; trustworthiness;
AI	Data computation; storage; modelling; collection and analytics; and programmability
ManyNets	Addressing; mobility; network interface; and heterogeneous network convergence

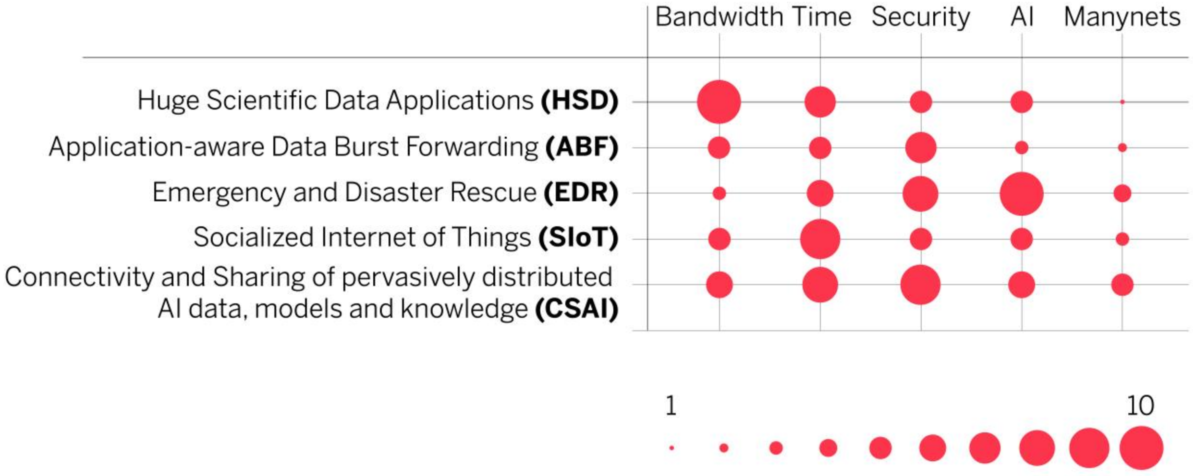


Figure 15 – Relative network requirement scores for the 5 representative use cases – ball diameter graph representation

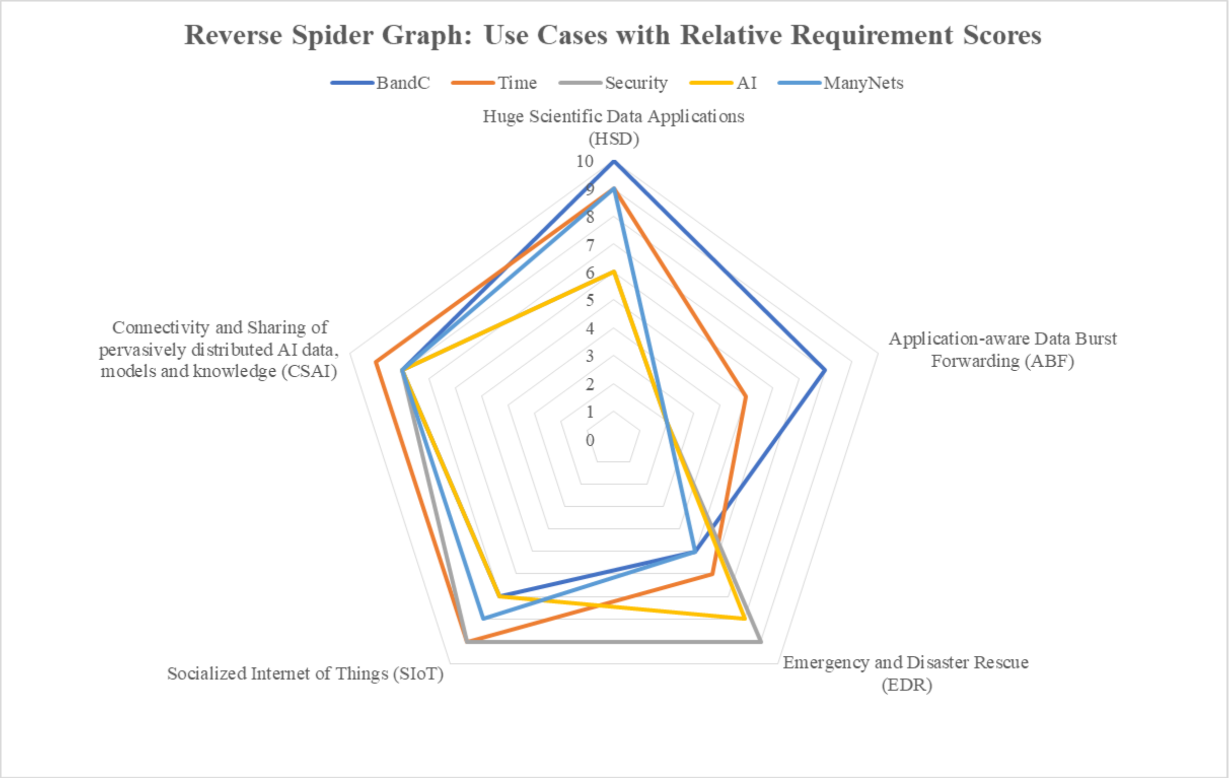


Figure 16 – Relative network requirement scores for the five representative use cases – reverse spider graph

In Figure 15, the relative importance of network requirements can be easily compared, horizontally for different dimensions of one particular case, or vertically for a specific dimension across multiple use cases. On the other hand, Figure 16 shows the relative significance of each network requirement dimension for a given use case, and the most prominent dimensions for all use cases.

Additionally, Figure 17 below collectively presents the relative importance of each of the five network requirement dimensions. This is consistent with the equivalent illustration in [34].

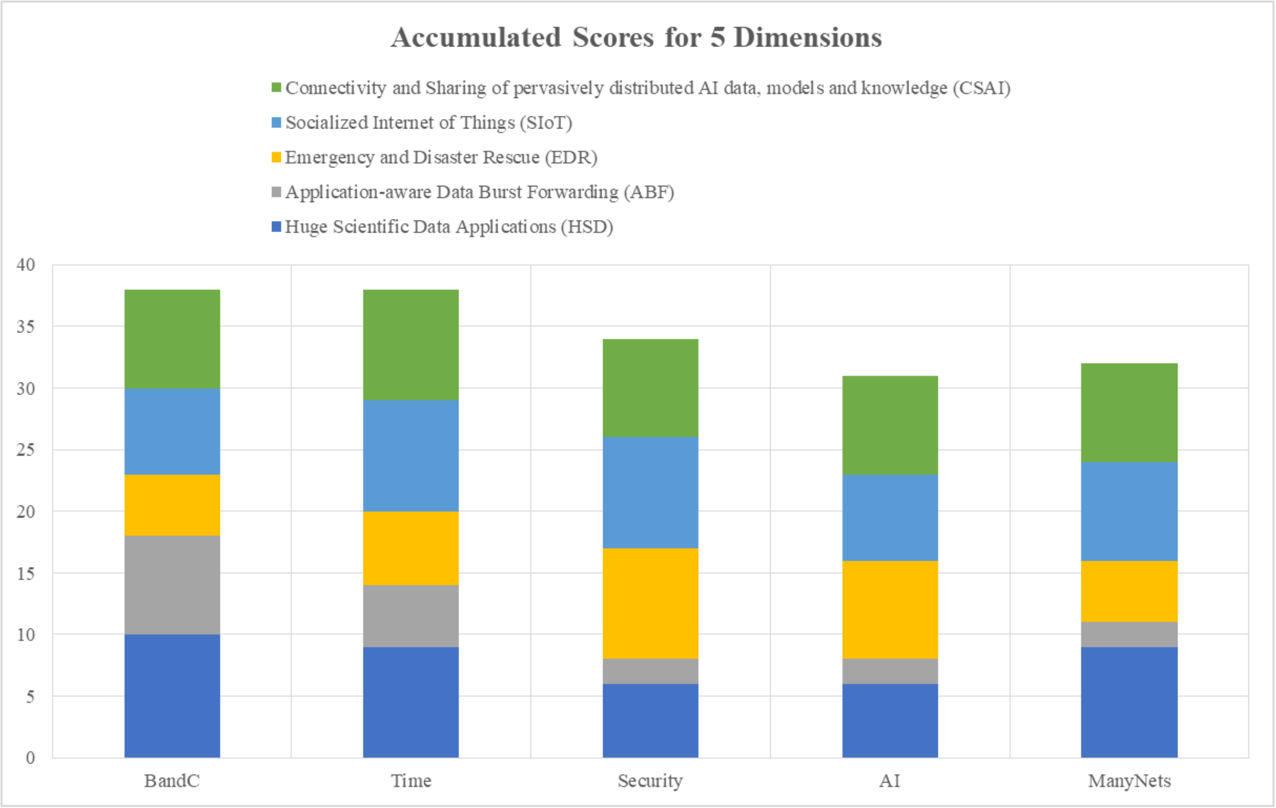


Figure 17 – Accumulated dimensional scores for the five representative use cases

II.2 The five abstract requirement dimensions and related analysis of the representative use cases for Network 2030

The representative use cases identified for Network 2030 each have their own requirements in terms of specific network capabilities. In order to plan the deployment of a specific service, it is important to understand its requirements at a high level as well as its impact upon the different dimensions. In simple terms, the views of all stakeholders, from network operators all the way through to end users, have to be considered: for example, bandwidth might be key to an end user's application flow, but an operator will be considering aggregated bandwidth and requirements of applications simultaneously using the network for multiple purposes.

In this context, each dimension adopted in Figures 15 and 16 has been abstracted after considering and consolidating different (but related) factors.

Table 4, in line with the use case descriptions in Part I, summarizes the scores of the five abstract requirement dimensions for each of the described use cases.

Table 4 – Abstract requirement dimension scores for the described use cases

Use cases	Bandwidth	Time	Security	AI	ManyNets
Huge Scientific Data Applications (HSD)	10	9	6	6	9
Application-aware Data Burst Forwarding (ABF)	8	5	2	2	2
Emergency and Disaster Rescue (EDR)	5	6	9	8	5
Socialized Internet of Things (SIoT)	7	9	9	7	8
Connectivity and Sharing of pervasively distributed AI data, models and knowledge (CSAI)	8	9	8	8	8

The following provides some considerations in terms of use case analysis with respect to each of the abstract requirement dimensions.

The **Bandwidth** dimension is one of the two highest score dimensions. The HSD, ABF and CSAI use cases imply a quite huge amount of transmitted data so that the bandwidth provides a basic support for these applications. Due to the foreseen large scale deployment of SIoT devices, the bandwidth is also a key parameter to be considered for the SIoT use cases.

The **Time** dimension is the other dimension with the highest scores. This dimension is very important for the HSD, SIoT and CSAI use cases, and this is not only in terms of end-to-end latency, but also in terms of jitter. For example, some of the HSD and CSAI applications need accurate data synchronization.

The **Security** dimension is very relevant in most of the use cases. EDR needs a network providing trustworthy infrastructure. For SIoT, the network needs to play a critical role in terms of overall security as most of the IoT devices are unable to shoulder adequate security capabilities. Adequate security and privacy are required for CSAI since most of the relevant information involved in this use case is associated with personal devices and their users. More generally, future networks need to increase their security and privacy protection capabilities.

The **Artificial Intelligence** (**AI**) dimension increases in relevance and practical impact upon applications almost on a daily basis. CSAI is a typical use case where AI plays a core role (optimization, prediction). It is believed that AI will play an important role in future networks.

The **ManyNets** dimension represents the heterogeneity score of the networks. The high score for the HSD use case is due to the heterogeneity of physical and logical patterns and scenarios in the scientific research area, requiring network capabilities in measure to support this diversity of network contexts. SIoT and CSAI are typical use cases that, from the viewpoint of large scale distribution of devices and capabilities, imply ubiquitous and seamless interworking of heterogeneous devices and networks.

Conclusion

Part I of this report on use cases and network requirements for Network 2030 describes five representative use cases for Network 2030 with their key network requirements. These use cases are additional ones with respect to those described in the previous report.

Part II summarizes the network requirements according to their relative importance with respect to five abstract dimensions, and the relative scores for each use case are also evaluated and illustrated graphically.

Collectively, and within the limits of this restricted exercise, it is believed that the representative use cases described in this second report may provide a potential vision of additional new applications and services in the era of Network 2030.

References

[1] Sub-Group 1's SharePoint page: https://extranet.itu.int/sites/itu-t/focusgroups/net-2030/SitePages/Sub-Group%201.aspx

[2] VLBI: http://www.jive.nl/e-vlbi

[3] SKA: https://australia.skatelescope.org/welcome/

[4] FAST: https://fast.bao.ac.cn/

[5] LHC: http://lhcone.web.cern.ch/

[6] ITER: https://www.iter.org/proj/inafewlines

[7] Yamanaka, Kenjiro, et al. "Long distance fast data transfer experiments for the ITER Remote Experiment." Fusion Engineering and Design 112 (2016): 1063-1067.

[8] Johnston, William E. "ESnet4: Advanced Networking and Services Supporting the Science Mission of DOE’s Office of Science." (2007).

[9] Y Chen, R Griffith, D Zats, A D Joseph, Understanding TCP Incast and Its Implications for Big Data Workloads, ;login: issue: June 2012, Volume 37, Number 3.

[10] Andrew S. Tanenbaum, David J. Wetherall (2011, Fifth Edition. International Edition), "Computer Networks". page 361 ISBN 978-0-13-255317-9.

[11] Katevenis, Manolis; Sidiropoulos, Stefanos; Courcoubetis, Costas (1 October 1991). "Weighted round-robin cell multiplexing in a general-purpose ATM switch chip". IEEE Journal on Selected Areas in Communications. 9 (8): 1265–1279. doi:10.1109/49.105173. ISSN 0733-8716.

[12] Adam Langley, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind, Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Ryan Hamilton, Victor Vasiliev, Wan-Teh Chang, and Zhongyi Shi. 2017. The QUIC Transport Protocol: Design and Internet-Scale Deployment. In Proceedings of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM '17). Association for Computing Machinery, New York, NY, USA, 183–196. DOI: https://doi.org/10.1145/3098822.3098842

[13] I. Rhee, etc., CUBIC for Fast Long-Distance Networks, RFC8312.

[14] Neal Cardwell, Yuchung Cheng, C. Stephen Gunn, Soheil Hassas Yeganeh, Van Jacobson, BBR: Congestion-Based Congestion Control, ACM Queue, Volume 14, issue 5

[15] H.T. Kung, T. Blackwell, and A. Chapman, "Credit-Based Flow Control for ATM Networks: Credit Update Protocol, Adaptive Credit Allocation, and Statistical Multiplexing," Proceedings of the ACM SIGCOMM 1994 Symposium on Communications Architectures, Protocols, and Applications, pp. 101-114, August 31-September 2, 1994.

[16] ITU-T draft Recommendation Y.smart-evacuation "Framework of Smart Evacuation during emergencies in Smart Cities and Communities" (Geneva, 4-15 September 2017)

[17] ITU-T draft Recommendation Y.disaster_notification "Framework of the disaster notification of the population in Smart Cities and Communities" (Cairo, 6-15 May 2018).

[18] One trillion new IoT devices will be produced by 2035, https://learn.arm.com/route-to-trillion-devices.html

[19] https://discover.dhl.com/content/dam/dhl/downloads/interim/full/dhl-trend-report-internet-of-things.pdf

[20] ITU-T Y.4102 (2015), Requirements for Internet of Things devices and operation of Internet of Things applications during disaster.

[21] ITU-T Y.4121 (2018), Requirements of an Internet of Things enabled network for support of applications for global processes of the Earth.

[22] ITU-T Y.2239 (2016), Requirements for information control network and related application.

[23] ITU-T Y.2221 (2010), Requirements for support of sensor control network (SCN) applications and services in the NGN environment.

[24] Knud Lasse Lueth, "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating," IoT Analytics, August 2018

[25] L. Atzori, A. Iera, and G. Morabito. The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. Computer Networks. 2012.

[26] E. Papagiannakopoulou, et al. The COG-LO Framework: IoT-based COGnitive Logistic Operations for next generation logistics. IEEE WF-IoT. 2019.

[27] L. Atzori, A. Iera, and G. Morabito. Sociocast: a new network primitive for the IoT. IEEE Communications Magazine. 2019.

[28] L. Atzori, C. Campolo, A. Iera, G. Milotta, G. Morabito, S. Quattropani. Sociocast: Design, Implementation and Experimentation of a New Communication Method for the Internet of Things. IEEE WF-IoT. 2019.

[23] https://www.gartner.com/en/documents/3956015/hype-cycle-for-emerging-technologies-2019

[30] https://www.idc.com/getdoc.jsp?containerId=US45575419

[31] Morabito, R., Farris, I., Iera, A., & Taleb, T. (2017). Evaluating performance of containerized IoT services for clustered devices at the network edge. IEEE Internet of Things Journal, 4(4), 1019-1030.

[32] Chen, M., Hao, Y., Hu, L., Hossain, M. S., & Ghoneim, A. (2018). Edge-CoCaCo: Toward joint optimization of computation, caching, and communication on edge cloud. IEEE Wireless Communications, 25(3), 21-27.

[33] Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. IEEE Communications Surveys & Tutorials, 20(4), 2923-2960.

[34] First Sub-G1 report on "Use cases and network requirements for Network 2030" (Jan 2020), https://www.itu.int/pub/T-FG-NET2030-2020-SUB.G1

Main contributors

- **Part I**:
  - **HSD case**: Yongmao Ren (CAS, China); Xu Zhou (CAS, China); Wanghong Yang (CAS, China); Pengfei Fan (CAS, China)
  - **ABF case**: Jingcheng Zhang (Huawei, China); Min Zha (Huawei, China); Bin Da (Huawei, China)
  - **EDR case**: Viliam Sarian (NIIR, Russia); Anatoly Nazarenko (NIIR, Russia)
  - **SIoT case**: L. Atzori (CNIT, Italy), A. Iera (CNIT, Italy), G. Morabito (CNIT, Italy).
  - **CSAI case**: L. Atzori (CNIT, Italy), C. Campolo (CNIT, Italy), A. Iera (CNIT, Italy), G. Morabito (CNIT, Italy)
- **Part II**: Shen Yan (Huawei, China); Bin Da (Huawei, China); Marco Carugi (Huawei, Europe); Sundeep Bhandari (NPL, UK)
- **Overall editing and coordination**: Shen Yan (Huawei, China); Bin Da (Huawei, China); Marco Carugi (Huawei, Europe); Sundeep Bhandari (NPL, UK); Daniel King (Lancaster University, UK)