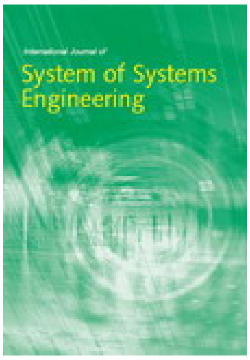


International Journal of System of Systems Engineering

ISSN online: 1748-068X - ISSN print: 1748-0671
https://www.inderscience.com/ijsse

On the interrelationship between IoT and SoS

Parisa Mahya, Hooman Tahayori, Mehrdad Tirandazian

DOI: 10.1504/IJSSE.2023.10051439

Article History:

Received:	28 October 2021
Accepted:	11 January 2022
Published online:	16 February 2023

On the interrelationship between IoT and SoS

Parisa Mahya and Hooman Tahayori*

Department of Computer Science and Engineering and IT,
Shiraz University,
Shiraz, 71438-51154, Iran
Email: parisa.mahya@gmail.com
Email: tahayori@shirazu.ac.ir
*Corresponding author

Mehrdad Tirandazian

School of Engineering Technology and Applied Science,
Centennial College,
Toronto, M1K 5E9, Canada,
Email: mtirandazian@centennialcollege.ca

Abstract: The rise and evolution of the internet on the one hand and complex systems on the other hand have led to a dense and distributed network of complex systems. Emergence of new technologies like internet of things (IoT) and system of systems (SoS) is a result of such widespread growth of internet and complex system structures. The distributed network of complex systems and their interactions are necessary to solve and tackle global problems. However, there are challenges in different aspects of complex systems like security, performance, and decision-making that need further investigation. This paper studies the relationship between IoT and SoS and discusses how IoT can be considered a subcategory of SoS. Since SoS is established to analyse and solve problems of complex and large systems and facilitates the challenges in related situations, IoT as a subcategory of SoS would benefit SoS toward systematic growth and efficient problem solving.

Keywords: SoS; system of systems; IoT; internet of things; microgrids; e-Health; smart transportation.

Reference to this paper should be made as follows: Mahya, P., Tahayori, H. and Tirandazian, M., (2023) 'On the interrelationship between IoT and SoS', *Int. J. System of Systems Engineering*, Vol. 13, No. 1, pp.50–65.

Biographical notes: Parisa Mahya received her Masters' degree in Software Engineering from Shiraz University, Iran. Currently, she is a PhD student at Johannes Kepler University, working on Explainable AI and interpretability. She is interested in the areas of IOT, SOS and the applications of data mining and machine learning algorithms.

Hooman Tahayori received his PhD in Informatics from the Universita Degli Studi di Milano, Milan, Italy, in 2009. He is currently an Associate Professor with the Department of Computer Science and Engineering and Information Technology, Shiraz University. He has authored or co-authored more than 60 technical papers in the areas of type-2 fuzzy sets, shadowed sets, granular computing, and perceptual computing. His main research interests include fuzzy sets of higher order, perceptual computing, granular computing, and their applications in various disciplines.

Mehrdad Tirandazian is a Professor in the School of Engineering Technology and Applied Science, at Centennial College. He has a PhD in Computer Science and more than ten years of experience in teaching and IT project management. His main areas of expertise include but not limited to software engineering, digital, mobile, and internet based media, fuzzy logic, computer graphics, simulation of discrete and continuous systems, VLSI design and optimisation. He is also involved in scholarly work and applied research through Centennial's Applied Research, Innovation and, Entrepreneurship Services (ARIES), and has developed various mobile and web based software applications. He is also an instructor of the Computer Science department at Ryerson University and Computer Engineering department at University of Ontario Institute of Technology.

This paper is a revised and expanded version of a paper entitled 'IoT is SOS' presented at the *International Conference on Internet Computing (ICOMP)*, Las Vegas, USA, 2016.

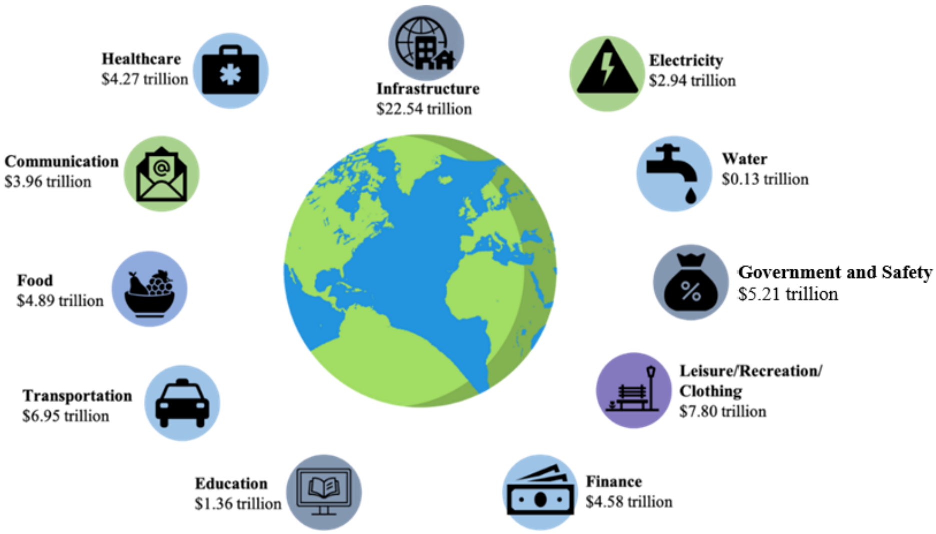
1 Introduction

World is consisted of 11 interrelated core systems including infrastructure, electricity, education, communication, water, transportation, leisure/recreation, healthcare, government and safety, food, and finance that are shown in Figure 1 (Korsten and Seider, 2010). Although each core system works independently and has its goals, objectives, and policies however, collaborations among the mentioned systems address the needs of society. For instance, food system without transportation and water systems cannot achieve its goals. Sustainable living demands for the optimisation of the behaviour of all mentioned core systems. What is important to notice is that, optimising an individual core system, without considering its relations with other systems, does not necessarily improve the efficiency of the whole system. Optimising food system, without improving transportation system, may frustrate water, infrastructure and transportation systems and negatively affect other systems. Resolving the inefficiencies in the world, requires considering and optimising all core systems together. Traditional optimisation strategies in this case does not work, instead, system of systems (SoS) view may take effect.

The presence and importance of complex systems in recent decades has led to the establishment of new research threads and technologies including SoS. SoS is a super system comprised of other elements which themselves are independent, complex operational systems that interact among themselves to achieve higher goals. In real world, a complex system can be a part of a larger network or be an object in the environment. In this case, new challenges and problems arise related to the objects and their interaction and communication, which allows them to act intelligently and share observations in real world.

SoS is primarily used in military and space shuttles' design and has wide variety of applications in security, aerospace, manufacturing, service industry, environmental system, and disaster management (Jamshidi, 2008). SoS has several benefits over regular systems. It provides high-level viewpoints among systems, and enables effective analyses and implementation of heterogeneous, independent, cooperative, and complex systems (Jamshidi, 2008).

Figure 1 11 core systems in the world (see online version for colours)



Source: Korsten and Seider (2010)

The objective of SoS is far beyond making decisions and predictions; it aims to attain clear understandings of problems and addressing the challenges in the whole system and bridging the gap between understanding and communication (DeLaurentis and Callaway, 2004). SoS has the ability to evaluate the probability of possible outcomes if a set of interrelated actions are triggered which is called the probability of possibility or what-if map (Chaudhuri, 2018). It is argued that the main cause of inefficiency of the complex systems, roots at the inappropriate and ineffective interrelationship among the systems (Korsten and Seider, 2010). It is believed that rapid development in sensors, actuators, processing power and communication can be helpful in making the interrelationship among the core systems intelligent and efficient.

The fundamental idea of IoT is based on the pervasive presence of objects around us that can interact with each other – via smart sensors, RFIDs, etc. – to achieve common goals. The existing technologies including RFID tagging, has posed IoT in various fields and areas such as healthcare, transportation, smart home, etc. IoT on one hand is a system that can facilitate interrelationship among other systems and hence can be considered as a system in an SoS. On the other hand, IoT itself can be considered as an SoS that is the topic of this paper. This paper, as an extension of Mahya and Tahayori (2016) demonstrates that IoT is a subcategory of SoS by providing evidences, investigating cases, and illustrating a comprehensive overview of IoT and SoS. In this paper we discuss a one-to-one relation between IoT and SoS. This view enables the design of any IoT more efficiently.

IoT consists of distributed smart devices with limited memory and processing capabilities, however huge amount of data is generated in IoT that handling them requires changing the traditional systems into IoT-enabled systems. This task is difficult since there are many factors and concepts that should be considered in the modification process. The important considerations are related to security, smartness, interoperability, and autonomy. Furthermore, as the nodes increase, it is necessary to define and use a scale-free topology that is flexible with the expansion of nodes. We demonstrate that the interconnections among the smart devices or smart systems would be easier to handle if it is observed from the SoS perspectives.

This paper is organised as follows. Section 2 reviews the definitions and characteristics of SoS. Section 3 explains various definitions of IoT, and Section 4 is dedicated to the relationship between IoT and SoS. Section 5 concludes the paper.

2 System of systems: definitions and characteristics

To contrast and compare SoS and IoT, initially we review different definitions, characteristics, and attributes of SoS. Many definitions are proposed for SoS which are reviewed below:

Definition 1: "System of Systems integration is a method to pursue development, integration interoperability and optimisation of systems to enhance performance in future battlefield scenarios" (Jamshidi, 2008).

Definition 2: "System of Systems are large-scale concurrent and distributed systems that are comprised of complex systems" (Jamshidi, 2008).

Definition 3: "Enterprise System of System Engineering (SoSE) is focused on coupling traditional systems, engineering activities of strategy planning and investment analysis" (Jamshidi, 2008).

Definition 4: "System of Systems is a multiple, independent systems that interact for the purpose of global goal" (Baldwin and Sauser, 2009).

Definition 5: "SoS is defined as a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities" (Firesmith, 2010).

Definition 6: "SoS [is a] collection of trans-domain networks of heterogeneous systems that are likely to exhibit operational and managerial independence, geographical distribution and emergent and evolutionary behaviours that would not be apparent if the systems and their interactions are modelled separately" (DeLaurentis and Callaway, 2004; Firesmith, 2010).

As mentioned earlier, there is not a unique definition for SoS that all researchers agree upon. However, to distinguish a normal system from SoS, several characteristics are counted and identified for SoS.

Seven attributes are proposed by Global Earth Observation System of Systems (GEOSS) for SoS. It is noteworthy to mention that GEOSS is a mission of Group on Earth Observation (GEO) with the aim of monitoring the state of earth and enhance the understanding of earth processes. The attributes can be counted as:

Operational independence, managerial independence, geographical distribution, emergent behaviour, evolutionary development, self-organisation, and adaptation. Since most references have considered first five attributes, in this paper we elaborate on them too.

Operational independence indicates independency and usefulness of subsystems such that each subsystem can operate while being detached from others. Managerial independence signifies that each subsystem can be managed according to its own policies and can operate autonomously. Geographical distribution refers to the ability of subsystems to communicate and interrelate while being geographically separate. Emergent behaviour states that the behaviour of a system is based on the relationship among its parts – than being simply the summation of the functionalities of individual parts. A collection of complex systems' properties is called emergent property that is not available in an individual system. Evolutionary behaviour is an indication that SoS evolves over time based on modifications and changes.

The Internet of Things (IoT) is an emerging technology that enables devices equipped with sensors to connect and interact with machines and humans via various networks.

The very first idea of IoT was presented in 1985 by Peter T. Lewis in a conference in which he used the term IoT to describe wireless connectivity of machines and devices. In his speech, he mentioned, "IoT is the integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such devices. In 1999, Kevin Ashton used the term IoT in the context of supply management. The main motivation of IoT was explained by Ashton as: "Today computers – and, therefore, the internet – are almost wholly dependent on human beings for information…. The problem is people have limited time, attention and accuracy… We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves…" (Wu et al., 2014)

In 2001, Auto-ID center in MIT represented a viewpoint of IoT as follows,

> "The Electronic Product Code (EPC) was conceived as a mean of identify all physical objects. The primary purpose of the EPC was to serve as a reference to networked information. Used in conjunction with Object Name Service, the EPC associates the physical object with information about the object. Together, these components allow physical objects to be networked, creating essentially as Internet of Things." (Brock, 2001)

IoT is changing rapidly with the aim of creating an integrated internet that evolves people's lives, thoughts and works. However, like SoS, there is no comprehensive definition for IoT.

According to Cisco, IoT is the "Internet of Everything" which links objects to the internet, enabling data and insights never available before (Chaudhuri, 2018).

McKinsey & Company defines IoT as "sensors and actuators connected by networks to computing systems. These systems can monitor or manage the health and actions of connected objects and machines. Connected sensors can also monitor the natural world, people and animals." (Chaudhuri, 2018)

IEEE has defined IoT as a network of items each embedded with sensors, which are connected to the internet (Minerva, 2016).

ETSI – a standardisation organisation in the telecommunication industry- has introduced machine-to-machine (M2M) concept that is like IoT. According to Singh et al. (2014) M2M is a communication between two or more entities that does not necessarily need any human direct intervention. Its services intend to automate decision and communication processes.

Internet Engineering Task Force (IETF) describes IoT as a basic idea that connects objects around us to provide seamless communication and contextual services provided by them (Minerva, 2016).

Another definition is presented by ITU, the United Nations specialised agency for information and communication technologies. ITU utilises the phrase ubiquitous network while defining IoT, which means the availability of networks everywhere and anytime (Singh et al., 2014).

OASIS, a nonprofit international consortium has defined IoT as a system where the internet is connected to the physical world via ubiquitous sensors. Sensing, efficient, networked, specialised and everywhere are known as the five key attributes that distinguish IoT from the regular internet (Chaudhuri, 2018)

2.1 Internet of things: philosophy

According to Floridi (2010), the philosophy of information is defined as "the philosophical field concerned with

a the critical investigation of the conceptual nature and basic principles of information, including its dynamics, utilisation, and sciences

b the elaboration and application of information-theoretical and computational methodologies to philosophical problems" (Mahmoud and Al-Sunni, 2015; Mahmoud et al., 2015).

To build trust in IoT technology, it is necessary to provide satisfactory answers to the techno-philosophical questions from users as depicted in Figure 2. The questions can be evaluated in five main dimensions as described in the following (Mahmoud and Al-Sunni, 2015; Chaudhuri, 2018).

1 *Ontology*: It is a systematic term of existence. In the context of knowledge, it means specification of a conceptualisation that explains what exists is what can be represented. In IoT technologies, ontology should describe the existence of IoT using the smart devices, network communication, applications, and data flow. In other words, for a new user in this technology, it should interpret and answer the question "what is IoT?"

2 *Phenomenology*: As Wilson stated, the goal of phenomenology is to "study how human phenomena are experienced in consciousness, in cognitive and perceptual acts, as well as how they may be valued or appreciated aesthetically. Phenomenology seeks to understand how persons construct meaning" (Chaudhuri, 2018). In the context of IoT, the question is "How do we experience it?". Obviously, the answer can be any IoT application including smart home and the sensors gathering data in the environment, the smart alert system that notify the police about crime or any security violation, etc. The phenomena of autonomous perception, intentionality and embodiment can be built through smart sensors. An example is the soil and air humidity sensors that auto-enable the watering systems in a garden.

3 *Epistemology*: This dimension asks the question "How do we know it?" and in IoT technology, this refers to the necessary technicalities and functionalities to develop a

trust or as it is called, epistemic trust and it can be satisfied through the interplay of technical aspect (techno-epistemic trust) and social aspect (social epistemology). In techno-epistemic trust, the users must assure that the output of Things in IoT is what it should be.

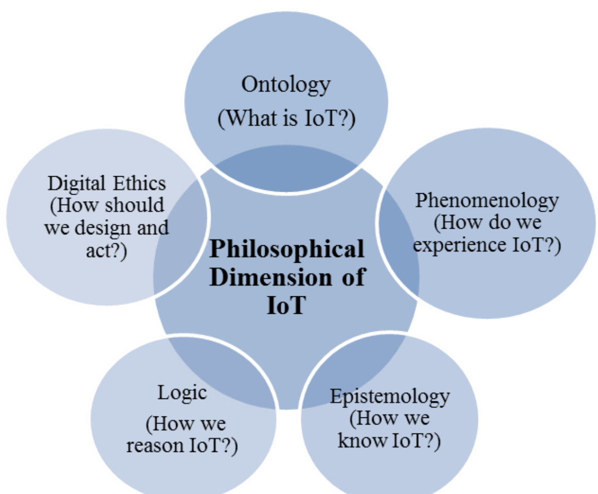
The interaction and usage of devices and applications gradually emerge the social dimension of IoT which requires to develop a social trust in knowledge development by human or non-human agents.

4 *Logic*: This dimension is aligned with the epistemology dimension and regarding output of IoT devices and applications asks about "How do we reason with it?"

The user tries to deduce the reason behind the generated output from smart devices and services and this reasoning process can happen through knowledge reference accessing, self-help guidance, etc.

5 *Digital ethics*: Ethics refers to "systemising, defending and recommending concepts of right and wrong behaviour" (Chaudhuri, 2018). In IoT technology, ethics ask "How should we design and interact with it?" (Chaudhuri, 2018) To answer this question, it is essential to define moral standards in IoT design and operation considering various terms and aspects such as security, reliability, regulatory, etc.

Figure 2 Five philosophical dimension of IoT technologies (see online version for colours)



Source: Mahmoud and Al-Sunni (2015)

2.2 Internet of things: architecture

IoT architecture is consisted of several key components as described in the following. (Chaudhuri, 2018)

- *Sensors and actuators*: based on the definition by IEEE a sensor is "an electronic device that produces electrical, optical or digital data derived from a physical condition or event. Data produced from sensors is then electronically transferred, by another device, into information (output) that is useful in decision making done by intelligent devices or individuals" (Chaudhuri, 2018).

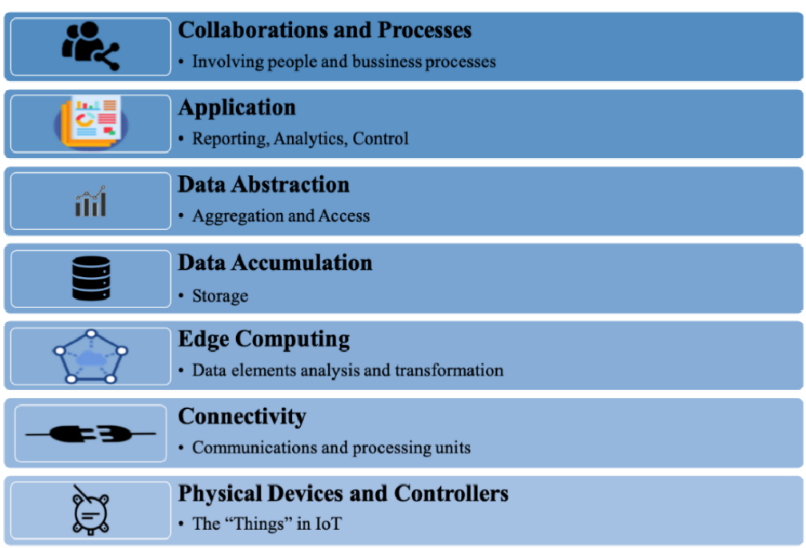
Sensors have different functionalities, and they are designed according to the needs and requirement such as temperature sensors, pressure sensors, smoke sensors, etc.

An actuator is "a mechanical device that accepts a data signal and performs an action based on that signal" (Chaudhuri, 2018)

- *Data communication media*: The communication among Things in IoT can be performed wired or wireless and there are variety of protocols to choose. The well-known ones are internet, Zigbee and Bluetooth Low Energy.
- *Storage*: The collected data can be stored locally on a smart device, or it can be sent to a cloud-based storage.
- *Control system*: is a part of operation center. Its duty is to check the relevance of collected data according to the requirements. If the data are in acceptable range and format, then the control system allows them to be saved for further processing. Otherwise, it sends a change instruction to the actuator and the sensors recollect the data according to new defined pattern and range.

To standardise the concept of IoT, a reference model is represented by the IoT World Forum as depicted in Figure 3. The model consists of seven layers and is based on information flow.

Figure 3 IoT reference model (see online version for colours)



Source: Chaudhuri (2018)

The first level, physical devices and controllers are the Things in IoT. They can communicate, to be controlled and generate data. The captured data are stored in a small unit in level 2 due to low storage. Level 2 should maintain the reliability of transmission.

In level 3, Edge (fog) Computing, the concept of fog computing is utilised to process the information with minimum latency in capturing data. In level 4, a conversion from event-based data in a network to data suitable for processing is performed. This may include sampling, event aggregation, filtering, etc. Level five creates schemas and views of data to simplify the access of data.

Level 6, namely application, is where the information can be interpreted according to specific application and the last level, collaboration and process makes the IoT application useful by dealing with people and business processes.

Generally, there are challenges to develop, modify, and implement traditional security techniques and methods in IoT. Most of the challenges are access control challenges that arise from the fact that IoT devices require low power and they are unable to perform complex encryption algorithms because of their memory limitation. Furthermore, the nodes and devices are distributed geographically and the interconnection among nodes, devices and gateways are huge and dense. These factors emerge the need to evaluate and create a SoS.

3 Internet of things vs. system of systems

Although few studies have been conducted on the relationship between IoT and SoS (Lukkien, 2016; Fortino et al., 2021; Alkhabbas et al., 2016), this paper tries to investigate this relationship by considering their concepts, architectures and characteristics as well as some real applications in the world and to show how the IoT applications can be extended to SoS.

Elaborating on the definitions presented in Section 2, and considering the five characteristics enumerated, SoS is consisted of independent systems that are interoperating with each other to fulfil common goals. IoT, however, consists of two parts, Internet and Things. According to IoT definitions, things are heterogenous objects with some capabilities

An essential concept in IoT is system thinking, which means that IoT as a complex system should be able to think and basically smart devices are able to satisfy such ability. However, the presence of sensors is not sufficient for a system to think and there should be some other units for processing data and learning. IoT on the other hand has four basic hardware units namely, sensors/actuators, processing unit, storage unit and communication unit that facilitate data collection, data processing, decision making and learning. Moreover, an operating system like TinyOs is designed for IoT to fulfil requirements such as high-level programming and reliability (Singh et al., 2014).

Based on the discussions in Sections 2 and 3, a collection of objects equipped with sensors interacts in complex manner with each other or they integrate with other complex systems. Furthermore, data from remote sensors in an IoT system can be integrated into decision-making support systems, power grids, telecommunication networks and clouds and construct a complex large-scale system. Like any system, such a system must be managed and monitored from different aspects like security, reliability, etc. which are not easy through IoT and it can be considered as SoS to help solving the mentioned challenges.

To map IoT concepts to SoS definitions, key characteristics of SoS which distinguish a regular system from SoS should be satisfied. In the following, two cases on transportation and healthcare are examined to better understand IoT applications and their relevance to SoS characteristics.

Case 1: Nowadays, in most of the cities, numerous alternatives of public transportation such as metro and bus are available that are aimed to ease people's life. However, at the same time vehicles have destructive effects on the environment. Studies have revealed that air pollution causes by vehicles are as dangerous as traffic accidents (Kyriazis et al., 2013). In this case, IoT helps create a smart environment, intelligent transportation system, and smart cities that at the very least minimises pollution and controls traffic. To implement IoT in transportation, vehicles, roads, and traffic lights should be equipped with sensors. Vehicles are systems themselves that operate independently while cooperating with other vehicles and systems. For example, a bus operation is based on its schedule; however, it should cooperate with other buses and vehicles or even should connect to other sources of transportation, data centers and clouds toward controlling the traffic. Table 1 contrasts transportation with SoS attributes.

Table 1 IoT smart transportation as SoS

SoS ***characteristics***	*IoT Smart* ***transportation***
Managerially and operationally independent	Vehicles such as metro or bus are independent systems that operate independently, helping people to commute
Geographical distribution	Metros and buses in any geographical location and distances can share their information
Emergent behaviour	V2V applications such as cooperative driving, warning, and prevention (Lukkien, 2016)
Evolutionary behaviour	Autonomous vehicles are evolving and new technologies are adding to the vehicles and roads which are part of evolutionary behaviour

As is shown in Table 1, in smart transportation, devices are managerially and operationally independent. Devices can exchange information via various protocols such as MQTT regardless of their location, so geographical distribution characteristic is supported.

Undoubtedly reaching the goal of IoT is only possible through the cooperation of all devices. Each individual system cannot achieve the goal associated with IoT, in other words, minimising pollution as a goal is an emergent property of this system. In Kyriazis et al. (2013) a system for transportation based on IoT is proposed that utilises information to learn from experiences and evolve over time.

Case 2: People's health status has always been noteworthy and as lifestyle has changed, healthcare has become more important. Consequently, many successful studies and research have been done in this field and one of the improvements is known as e-Health (Li et al., 2021). Many definitions are presented for e-Health and some of them are related to the use of internet in healthcare and many attempts have been made in this direction (Fernandez and Pallis, 2014; Gong et al., 2015). An e-health framework based on IoT is proposed in Bui and Zorzi (2011) that has focused on increasing the quality of life especially for people with chronic diseases and emergency. In this paper, the authors illustrate a day of a diabetic person. Based on this scenario, low-cost medical devices equipped with sensors, communicates wirelessly, given a connection be available. They monitor the person's health status since a diabetic person needs special cares. In emergency, medical centers are alerted and will send services to the patients as soon as possible.

In this case, devices for general health monitoring work independently, measuring blood pressure and monitoring other vital signs, so they are managerially and operationally independent. Healthcare centers, devices and doctors are distributed in an IoT healthcare system so data can be shared via communications protocols in any geographical distribution – which coincides with the geographical distribution characteristic in SoS. Data obtained from health centers and systems can be used to track the quality of care and services to the patients and insurance companies can evaluate whether the quality meets the standards, which satisfy the emergent behaviour characteristics of SoS. Decisions about person's health status are made based on information in databases and new data can be added in the database that causes gradual changes and improvements in decisions, devices and medical instruments are developing to employ sensor and mobile technologies – which is evolutionary behaviour characteristics (Wickramasinghe et al., 2014). Table 2 contrasts this IoT case with SoS characteristics.

Table 2 IoT healthcare as SoS

*SoS **characteristics***	*IoT e-health*
Managerially and operationally independent	General health monitoring systems and devices are independent. They work independently with the goal of serving patient needs. They also have managerial independence and can operate in private sector, governmental management, etc. (Wickramasinghe et al., 2014)
Geographical distribution	Healthcare and centers are inherently distributed so they can communicate and share their data via communication protocols (Wickramasinghe et al., 2014)
Emergent behavio**u**r	Tracking the quality of services to the patients can be considered as one of the emergent behaviour (Wickramasinghe et al., 2014)
Evolutionary behavio**ur**	New drugs and devices that are evolving to employ new technologies such as sensors and they are part of evolutionary behaviour (Wickramasinghe et al., 2014)

As mentioned, objects in IoT are independent and operate independently. Furthermore, IoT is based on the internet and nowadays the internet is public, cooperative facility accessible to millions of people worldwide and is evolving over the years. So, it is easy to connect objects everywhere, anytime over the internet. In addition, as IETF has mentioned while defining IoT, objects cooperate with each other to make an accessible service from anywhere and anytime. (Minerva, 2016)

The fourth attribute of SoS, i.e., emergent behaviour, is satisfied in IoT since the heart of system thinking is an emergent property of the whole structure. In the previous cases, goals such as controlling traffic is only possible through interactions and cooperation among appliances and this is correspondent with the definition of emergent properties.

3.1 Microgrid

In this section, to prove that the relation between IoT and SoS is one way, we will show that not every SoS equipped with sensors, actuators, and processing and communication facilities can be considered as IoT.

Energy related issues have gained an increasing attention in recent decades because of increasing demands and unstable sources of energy. Thus, many research and studies have been conducted on managing and saving energy in different levels. Microgrid is a noteworthy part of the energy supply system that diminish pressure on main grids by generating energy in local areas.

Microgrid is a collection of small-scale, low-voltage electric power grid that can operate independently (island) or in conjunction with area's main electrical grid to meet the power requirements of a designated community. Like power grids, microgrids have their own sources and loads (Jamshidi, 2008; Mahmoud and Al-Sunni, 2015). More precisely, microgrids are kinds of backup to the main power grids during heavy demand periods. Due to the use of renewable sources of energy in microgrids, the cost of generating energy is reduced meanwhile they provide more reliable energy sources (Jamshidi, 2008). In order to achieve the mentioned goals in such complex systems and making the microgrids operate accurately and uninterruptedly, an appropriate architecture and model should be developed. As traditional methodologies for systems are not adequate and satisfactory, different models, architectures and methodologies are proposed based on SoS (Mahmoud et al., 2015; Mahmoud et al., 2015). In the following, the complexities and problems in microgrids are discussed and investigated from SoS perspective.

According to Zpryme/IEEE reports, three top industries that most likely tend to deploy microgrids are healthcare/hospital, government and utilities (Alford et al., 2012). U.S. Department of Defense (DOD) has been leading in deploying microgrids because of emergent needs and reliability of military to local power and electricity (Hayden and Ceh, 2013).

According to the U.S. Department of Energy (DOE) a micro grid, as a local energy network, offers integration of distributed energy resources (DER) with local elastic loads, which is able to operate in parallel with the grid or in an intentional island mode to provide a customised level of high reliability and resilience to grid disturbance. This advanced, integrated distribution system addresses the needs in locations with electric supply or delivery constraints, in remote sites, and for protection of critical loads as well as economically sensitive development (Myles et al., 2011).

A brief description of micro grid proposed by the Microgrid Exchange Group, states that a microgrid is a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island-mode (Bossart, 2012). Upon the aforementioned descriptions there exists several fundamental features in microgrids including:

- Island and grid connected operation mode
- combination of power generation sources and loads
- providing different levels of power quality and reliability for the end use.

The microgrids include distributed generation (DG), smart meters, power systems (PS) such as solar photovoltaics (PV), storage devices, management operation and control system (MOCS) which incorporate cybersecurity, decision making, modelling, prediction, optimisation and communication (Jamshidi, 2008; Mahmoud et al., 2015). From SoS perspective, microgrid satisfies all SoS characteristics.

All the components and subsystems in microgrid operate independently without interfering with other components. They rely on their own sources to produce energy and are responsible for their operations that corresponds to the managerial/operational independent characteristic (Mahmoud and Al-Sunni, 2015; Rainey and Tolk, 2015).

New devices and systems can be added to microgrids based on the emergent needs and according to modularity i.e., microgrids can be extended gradually and modernise the existing grids over time. This means that the overall system can develop and evolve gradually which corresponds to evolutionary behaviour (Mahmoud and Al-Sunni, 2015; Rainey and Tolk, 2015).

Furthermore, microgrid satisfies geographical distribution since the devices and subsystems can be distributed in different regions (Mahmoud and Al-Sunni, 2015; Rainey and Tolk, 2015).

In a microgrid, a straightforward managing goal such as deciding when to commit or start up a generator is a complex task that requires data from power network (Jamshidi, 2008). The worse stance is about detecting and monitoring unusual behaviours and faults in the systems that necessitate sensor meters to measure and evaluate customers' consumptions and patterns (Rainey and Tolk, 2015). Furthermore, the control system requires plenty of resources in order to communicate, send and receive information.

Accordingly, the challenges in microgrids are divided into two categories: technical and non-technical. The major challenges are related to current controlled (CC) which is a vital subsystem in microgrid. The main goal of CC is to supply power continuously without being affected by the changes in the system (Ustun et al., 2011). Challenges in mentioned subsystems can be about scheduling, protection, power quality, reliability, and stability.

As mentioned, microgrids operate in two modes. Normally they cooperate with main grids, however they can switch to island mode because of voltage drops, faults, etc. (Nigim and Lee, 2007). During the switching i.e., disconnecting from main grid, the controller should maintain an acceptable range of frequency and voltage for loads. From protection perspective, speed is an important factor in this situation since it is necessary to minimise the voltage-dip duration and guarantee stability. Generally, it is the duty of protection system to isolate the microgrid from the main grid at the time of fault occurrence (Kaur et al., 2016; Laaksonen, 2010).

Another problem is related to the control of huge number of micro sources. Precisely, after any failure or disconnection – which is inevitable – the system should have the ability to reconnect autonomously. Scheduling is another important issue that affects reliability and new methods should be proposed for prediction and forecasting (Nigim and Lee, 2007).

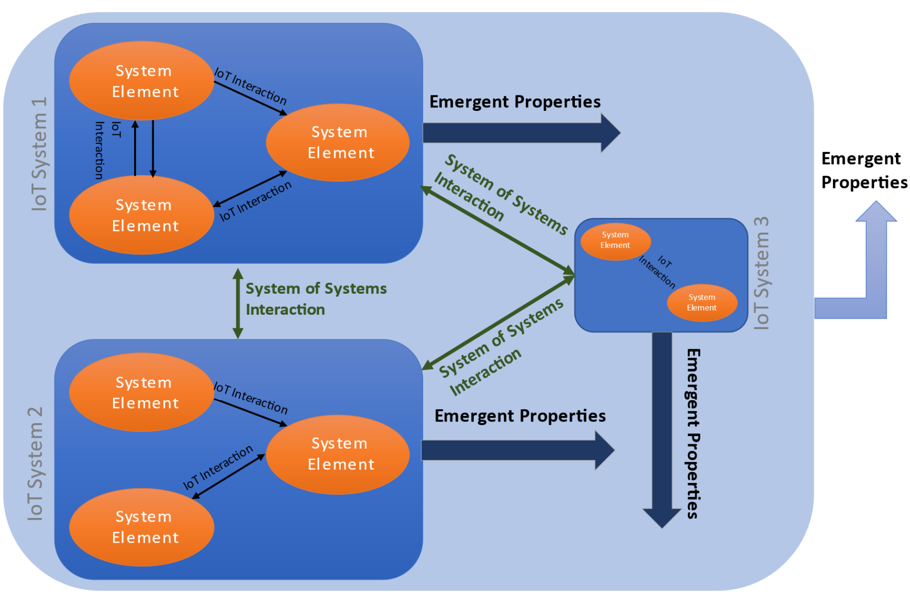
To overcome the mentioned issues and challenges, the whole microgrid system should be considered beyond the simple devices and things. This approach is possible if microgrid is considered as an SoS. Although, microgrid uses numerous sensors, and actuators but such devices constitute an IoT that facilitates the communications and interactions among the systems in the microgrid. Notably, when the application area enlarges determining the global requirements and the corresponding local actions are of utmost importance (Jamshidi, 2008). Hence, IoT would be exploited as a part of the solution or more precisely as a system that helps other components to better communicate and interact. It is clear that in such applications, IoT per se cannot be a solution to the problems like security, complex decision-making process, monitoring and maintenance. Microgrid satisfies all the requirements and characteristics of SoS and its architecture can be based on the SoS principles (Mahmoud et al., 2015) where IoT would one of its constituting systems.

4 Conclusion

In recent decades we have witnessed the development of many large systems. SoS, is devoted to study, analyse, design and implementation of systems composed of heterogenous, independent, cooperative, and complex systems. SoS can be considered as a multi-disciplinary study that has abstracted principles of developing large systems from different fields. Hence, putting any system under the umbrella of SoS facilitates applying the SoS principles that are adopted from other fields on that system.

In this paper we discussed that IoT is an SoS – but not vice versa – through studying the main characteristics of SoS that are present in IoT. IoT is consisted of many heterogenous devices that are geographically distributed, and each device can operate and manage independently. Things in IoT, introduce emergent behaviours that is truly beyond the summation of their capabilities and through the possibility of learning in IoT they depict evolutionary development. In a larger IoT application where the memory limitation, security, distribution, etc. matters, viewing them all through the SoS perspective would provide a more efficient solution.

Figure 4 IoT is a subcategory of SoS (see online version for colours)



Inspired by Jamshidi (2008) the concept of SoS while constructed from IoT is shown in Figure 4. The SoS consists of a multiple IoT subsystem, each of them with their own goals, subsystems, and emergent properties. While the IoT subsystems operate independently and perform their own tasks, they are part of the bigger system, i.e., SoS and their interaction with each other creates a higher-level goals and emergent properties.

In this paper we discussed a one-to-one relation between IoT and SoS, which would help in two folds. On the one hand, it enables viewing IoT as an SoS that helps alleviating more inefficiencies that normally occur with large number of constituting elements of complex systems. On the other hand, to optimise the performance of an SoS, an IoT can be developed to facilitate interactions, interrelations, and communications among constituting systems of the SoS, and hence as an autonomous system can be considered as a part of the SoS.

References

Alford, R., Dean, M., Hoontrakul, P. and Smith, P. (2012) *Power Systems of the Future: The Case for Energy Sotrage, Distributed Generation, and Microgrids*, Zpryme Research, and Consulting, Tech. Rep.

Alkhabbas, F., Spalazzese, R. and Davidsson, P. (2016) 'IoT-based systems of systems', *Proceedings of the 2nd Edition of Swedish Workshop on the Engineering of Systems of Systems (SWESOS 2016)*, Gothenburg, Sweden, pp.34–37.

Baldwin, W.C. and Sauser, B. (2009) 'Modeling the characteristics of system of systems', *2009 IEEE International Conference on System of Systems Engineering (SoSE)*, Albuquerque, NM, USA, pp.1–6.

Bossart, S. (2012) 'DOE perspective on microgrids', *Advanced Microgrid Concepts and Technologies Workshop*, Beltsville, MD, USA, pp.1–27.

Brock, D. (2001) *The Compact Electronic Product Code–a 64-Bit Representation of the Electronic Product Code*, White Paper, Auto-ID Center, November, Vol. 1.

Bui, N. and Zorzi, M. (2011) 'Health care applications: a solution based on the internet of things', *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, Barcelona, Spain, pp.1–5.

Chaudhuri, A. (2018) *Internet of Things, for Things, and by Things*, Auerbach Publications, New York.

DeLaurentis, D. and Callaway, R.K. (2004) 'A system-of-systems perspective for public policy decisions', *Review of Policy Research*, Vol. 21, pp.829–837.

Fernandez, F. and Pallis, G.C. (2014) 'Opportunities and challenges of the internet of things for healthcare: systems engineering perspective', *2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, Athens, Greece, pp.263–266.

Firesmith, D. (2010) *Profiling Systems using the Defining Characteristics of Systems of Systems (SoS)*, Software Engineering Institute, Carnegie Mellon University.

Floridi, L. (2010) 'The philosophy of information: ten years later', *Metaphilosophy*, Vol. 41, pp.402–419.

Fortino, G., Savaglio, C., Spezzano, G. and Zhou, M. (2021) 'Internet of things as system of systems: a review of methodologies, frameworks, platforms, and tools', *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 51, pp.223–236.

Gong, T., Huang, H., Li, P., Zhang, K. and Jiang, H. (2015) 'A medical healthcare system for privacy protection based on IoT', *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, Nanjing, China, pp.217–222.

Hayden, E. and Ceh, C. (2013) *Introduction to Microgrids*, Securicon Report, pp.1–13.

Jamshidi, M. (2008) *Systems of Systems Engineering: Principles and Applications*, CRC Press, Boca Raton, FL, USA.

Kaur, A., Kaushal, J. and Basak, P. (2016) 'A review on microgrid central controller', *Renewable and Sustainable Energy Reviews*, Vol. 55, pp.338–345.

Korsten, P. and Seider, C. (2010) *The World's 4 trillion Dollar Challenge: Using a System-of-Systems Approach to Build a Smarter Planet*, IBM Institute for Business Value, January.

Kyriazis, D., Varvarigou, T., White, D., Rossi, A. and Cooper, J. (2013) 'Sustainable smart city IoT applications: heat and electricity management, and eco-conscious cruise control for public transportation', *2013 IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Madrid, Spain, pp.1–5.

Laaksonen, H.J. (2010) 'Protection principles for future microgrids', *IEEE Transactions on Power Electronics*, Vol. 25, pp.2910–2918.

Li, X., Lu, Y., Fu, X. and Qi, Y. (2021) 'Building the internet of things platform for smart maternal healthcare services with wearable devices and cloud computing', *Future Generation Computer Systems*, Vol. 118, pp.282–296.

Lukkien, J. (2016) 'A systems of systems perspective on the internet of things', *SIGBED Rev.*, Vol. 13, August, pp.56–62.

Mahmoud, M.S. and Al-Sunni, F.M. (2015) 'A system of systems framework for microgrids', *Control and Optimization of Distributed Generation Systems*, Power Systems, Springer, Cham.

Mahmoud, M.S., Rahman, M.S.U. and Al-Sunni, F.M. (2015) 'Networked control of microgrid system of systems', *International Journal of Systems Science*, Vol. 47, No. 11, pp.2607–2619.

Mahmoud, M.S., Rahman, M.S.U. and Fouad, M.A., L-S. (2015) 'Review of microgrid architectures–a system of systems perspective', *IET Renewable Power Generation*, Vol. 9, pp.1064–1078.

Mahya, P. and Tahayori, H. (2016) 'IoT is SoS', *Proceedings on the International Conference on Internet Computing (ICOMP)*, Las Vegass, USA, pp.38–42.

Minerva, R. (2016) *Toward a Definition of Internet of Things*, IEEE IoT Initiative Chair, iot.ieee.org, Telecom Italia Research Centers (TIMLab), June.

Myles, P., Miller, J., Knudsen, S. and Grabowski, T. (2011) *430.01*.03 *Electric Power System Asset Optimization*, National Energy Technology Laboratory, Vol. 22, Morgantown, WV.

Nigim, K.A. and Lee, W-J. (2007) 'Micro grid integration opportunities and challenges', *Power Engineering Society General Meeting 2007*, IEEE, Tampa, FL, USA, pp.1–6.

Rainey, L.B. and Tolk, A. (2015) *Modeling and Simulation Support for System of Systems Engineering Applications*, John Wiley & Sons, Hoboken, New Jersey, USA.

Singh, D., Tripathi, G. and Jara, A.J. (2014) 'A survey of internet-of-things: future vision, architecture, challenges and services', *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, South Korea, pp.287–292.

Ustun, T.S., Ozansoy, C. and Zayegh, A. (2011) 'Recent developments in microgrids and example cases around the world_A review', *Renewable and Sustainable Energy Reviews*, Vol. 15, pp.4030–4041.

Wickramasinghe, N., Al-Hakim, L., Gonzalez, C. and Tan, J. (2014) *Lean Thinking for Healthcare*, Springer, New York, USA.

Wu, Q., Ding, G., Xu, Y., Feng, S., Du, Z., Wang, J. and Long, K. (2014) 'Cognitive internet of things: a new paradigm beyond connection', *IEEE Internet of Things Journal*, Vol. 1, pp.129–143.