Possibility of Internet of things technology implementation in smart power grids

Author: Krzysztof Billewicz - Politechnika Wrocławska

("Energetyka" - 5/2016)

The Polish power engineering regulatory ofce guidance assumes that implementation of smart metering in Poland should ensure the possibility of a new near-power-engineering services development, provided by companies from outside of the power engineering business with the use of Internet of Things technology [8]. In 2012, the Internet of Things (IoT) technology was recognized by the Polish energy regulatory ofce as a long-range goal in scope of its usage in smart power grids.

Available articles show that the Internet of Things (IoT) technology can be utilized for currently available smart power grids solutions development [3, 4].

The article proposes a division of Internet of Things concept into three groups, followed by presentation of possible implementation of this technology into various smart grid areas.

Defnition

In 1999 Kevin Ashton proposed to use a new term – Internet of Things. The Internet of Things (IoT) means that the surrounding devices can communicate with each other and also measure and define various properties and aspects of surrounding environment such as temperature, lighting, persons and objects presence detection, etc. Thanks to this the devices will become sources of various new information about the surrounding world. Currently, most of the information available in the internet is produced by people while in future, thanks to IoT technology, most of the information will be produced by machines (devices).

The Internet of Things is available with the use of electronic devices, various sensors and wireless communication technologies. The Internet of Things may be nearly limitless both in terms of size i.e. the number of interconnected devices as well as in terms of types of devices and collected data. The Internet of Things would encode about 50 to 100 trillion objects and be able to follow the movement of those objects.

The Internet of Things will include thermometers, sensors, smart energy meters, intelligent electronic devices, digital cameras and many more.

The IoT may become the biggest technological breakthrough in the network history.

The term Internet of Things is understood very differently by various researchers. There are three concepts which significantly differ from each other although are not mutually exclusive.

These are three categories-definitions:

- smart objects/devices
- smart sensors
- tags

Internet of things - smart objects/devices

The Internet of smart objects or devices - many intelligent devices will be connected to the global Internet network. In this definition the Internet of Things is a dynamical computer networks' application extension which will allow not only communication between people, but also between devices. Individual devices, e.g. home appliances like washing machines, dishwashers, fridges, dryers, thermostats and lighting, that up to now have not been computerized or connected to the Internet yet, will be equipped with computers. Such devices will communicate with each other without any human help or influence.

It seems that a particular challenge will be connected with smart devices firmware upgrade, because the operating system used in such devices can contain security vulnerabilities. A dilemma also appears, what to do if a producer of an operating system utilized in millions of devices would stop at a certain point of time trying to support that system by preparing software updates and patches for security vulnerabilities. In such case the device can stop working in a correct way.

Because devices will be equipped with various types of sensors, it will be possible to diagnose working status of each of them, inform about potential damages and even indicate the damaged spots. Such sensors can also prevent from a damage, e.g. switching of the devices in case the measured parameters limit values are exceeded - for example the temperature.

In such definition the Internet of Things is based on three main bases:

- identification (everything is capable of introducing itself),
- communication (everything can communicate with other things),
- cooperation (everything can interact with other things).

Objects surrounding us, e.g. being part of home appliances or road infrastructure buildings, will cooperate with personal belongings such as shoes, umbrellas, coats or glasses and with things that we own like TV sets, cars, ovens or fridges. This concept seems to dominate nowadays.

But the main question to ask is how to ensure a reliable power supply for smart devices in future?

Internet of things – smart sensors

The Internet of Things relies on placing very many intelligent sensors and detectors (smart sensors) in the environment – they would gather information unavailable up to now and would give access to it and its processing. Such sensors and the whole Internet of Things will be largely integrated with the environment. At now, sensors do not communicate with each other. For an example, in a car the sensor would detect low tire pressure and inform the driver about it. In case of a very low tire pressure the car would not move at all or could drive with a very low speed only, just to get to the nearest car service.

In relation to smart grids technology IoT means installation and gathering information from a large number of sensors. Such sensors would be used for a power fow monitoring and power network state monitoring (voltage stability, stability margin) as well as for individual devices state monitoring – power network elements e.g. transformers or circuit breakers. Thanks to adequate information it would be possible to predict earlier failure occurrence e.g. from ageing transformer oil, etc. In this concept we usually assume that the sensors do not communicate with each other – they do not contain executive elements, decision making algorithms or logics telling them which things they should connect with and for what purpose: which information to pass on and which to receive.

All signals and data coming from smart sensors will be data stamped with large accuracy, thanks to time module e.g. GPS signal.

Internet of things – tags

It relies on placing various tags, chips or microchips inside objects. Tags are small devices (microscopic computer chips) which allow positioning of those objects in space. Equipping very many objects in the world with small tags, indicating their position and identifying for reading would change our everyday life. The tags would also be placed on humans and animals and mostly the radio-frequency identifcation (RFID) technology will be used for it. Obviously, also Quick Response Code (QR), Barcodes, Near Field Communication (NFC) technologies etc. can be used here. Based on those identif-ers there can be performed operations like movement and presence detection or individual people or objects movement tracking. Based on this there would be prepared behavioral and habitual algorithms. On the grounds of such detection adequate systems in an intelligent home can inform about missing things or prepare shopping lists for a grocery shop or a drugstore. It can also order the missing products by itself. For example an intelligent refrigerator can read the RFID tags on products, see what kind of products are placed inside and inform the owners which product is nearing its expiry date. The intelligent refrigerator can monitor the nourishment habits of the owners, inform if they are right or wrong, how to eat in a healthy way, how many products are needed to be bought and whether the food supply will be enough for the coming weekend [2].

The concept, in which it is assumed that all devices can be connected to the Internet/network with radio communication of low power consumption is the most active research area in the

Internet of Things. In this concept individual tags do not communicate with each other. Such technology in smart grids area would be used „in places, where people are", so the main application would be for a home area network. It would be mostly used for people, products and cars presence monitoring.

RFID tags on nutritional products, clothes, drugs will not show up in the near future. And without the possibility of precise object identification it is hard to talk about tracking their movement and exact, clear identification.

Fog computing

The term Fog Computing was introduced by Cisco Systems Company, as a new paradigm of supporting wireless data transmission to support distributed devices in the Internet of Things concept. The Fog Computing (FG) extends the Cloud Computing (CC) paradigm to the edge of the network, thus enabling a new breed of applications and services.

Fog computing is a virtual platform that provides cloud computing capabilities, cloud storage and network services between end devices and a traditional data center cloud computing.

The fog computing is a new concept that can integrate cloud computing with the dynamically evolving IoT environment. The aim of fog computing introduction is to create an environment capable of gathering, storage and processing of large amounts of data (Big data) from millions of devices scattered in space and their delivery to the network borders. Such data, gathered from hundred thousands of sensors working in distributed network environment of IoT, will be supplied frstly to specialized border routers which after data preprocessing will direct them to further processing in specialized applications run in data centers [11].

We can simply say that fog computing can enable realization of Internet of Things and arrange in order the data gathered by many devices and sensors. A fog computing will allow the ubiquitous computing (allowing data to become available from any place and at any time).

The fog is in some sense a separated distributed network, found behind the routers. So, in case of fog computing, the key problems are:

- Data entrance from IoT into the cloud through the fog-border routers,
- Handling large amounts of data, putting them in order and processing,
- General access to the data or their input/output from the fog/ cloud to intelligent devices, dedicated systems or by a user request.

The critical issue seems to be the time of acquisition, data processing and access to the data and the bandwidth of both the network as well as routers located on the border of wide area of Internet and cloud-based shared services. The border routers will have to be able to receive very large amounts of data from many devices. Large amounts of data streams will have to pass through such routers to get to the computing fog/cloud [12].

Particular challenges will also concern [4]:

• guarantee of dynamic resources allocation – they will be assigned automatically, without human intervention,
• guarantee of reliable operation of the equipment, software, data and network resources that will be needed to prepare the service for a particular user,
• guarantee of network services reliability (allocation of resources, planning),
• guarantee of reliability of networks supporting data transfer and exchange of signals, messages and information on events.

Fog computing will be based on local computational resources and not, as it is in the case of cloud computing service, located somewhere in a remote place. This processing will provide greater security and greater efficiency. Fog computing is a distributed computing infrastructure.

Fog was brought to life to respond to the needs of a user who requests access to a large amount of data from any device, from any place and at any time.

Distinguishing features of fog computing are proximity to the end user, dense geographical distribution and support of mobile technologies. Fog supports densely distributed points of data collection. Fog devices are dispersed over a certain geographical area. With a wide geographical dispersal of fog its paradigm is well prepared for processing and analysing of large amounts of data in the real time.

In the Internet of Things the most difficult thing may seem to be the access to a device and fog computing is a concept that should simplify or even allow such an access. In addition, the intention is to be able to control a huge amount of data, be able to collect them within a reasonable time and allow a quick search and access to the data that are exactly needed. The challenge is to link a large number of devices with the network of data centers that can analyse such data, process them and expose the results of analyses and calculations. Moreover, there occurs a problem of huge amounts of data that may never be needed but will be read, processed and stored, occupying a lot of space.

Fog computing is supposed to make it possible to combine and integrate various industrial information systems - specialized and sectoral. The obtained data, using a variety of communication technologies such as ZigBee, Bluetooth or Z-Wave, will be transferred to a distributed computing infrastructure [1].

In fog computing, in a distributed computing infrastructure, it is to be guaranteed that the data obtained from the Internet of Things will be sent as expected while fully ensuring the confidentiality of some of these data. This is especially useful in situations where sensor data cannot be transferred across country borders for legal or regulatory reasons, which is now a very common problem in the implemented computing clouds [1].

Cyber security of internet of things

Undoubtedly, in the case of the concept of fog computing a serious problem will arise with:

- identification – how to identify a particular user,
- authorization – what entity should perform the authentication,
- access control – the basis on which it can be specified which resources, data files or devices a user or a thing is to be granted access to and to which he/it should have no access at all.

If a user is using a firewall, that significantly reduces the amount of data available about the user of the device in a computer network, then such an identification can be very dificult. One user can have many IP addresses (also many unique MAC addresses), as well as one computer and one IP address can be used by many users. So the identification must not be based on MAC address or IP device [10].

The matter of safety, security and reliability of access is also undeniable. This problem occurs with multiple applications. If an unauthorized person attempts to authorize access to resources by claiming to be someone else and entering the wrong password, it can lead to a temporary limit of service access availability. For example it won't be possible to log into the given service for a period of 10 minutes. In this way, the cybercriminal can maliciously block access to important services or important resources. Therefore, it is necessary to consider other types of security measures that will guarantee access to needed services „on demand". And similarly, the applied security methods must not cause periodical unavailability of allowance to contact with a certain thing/device.

Ensuring safety for new devices connected to the Internet is becoming a significant challenge. Bigger number of devices connected with the network ofer a lot more opportunities for a hacker attack and potential consequences of such actions. These are also new methods of spying on other people or stealing data. Currently, most of these devices are not protected against cyber-attacks. They also do not protect your privacy.

Internet of things in smart power grids

Many sensors will be located in a power grid. In order to ensure reliable operation of the power grid it will be needed to receive reliable and fast data from those sensors, processing of the data and application of appropriate control signals to actuators.

Internet of things can be used for smart power grids in the following areas:

- Internet of things for a smart city;
- Internet of things for smart metering;
- Internet of things for transmission and distribution power grids;
- Internet of things for an asset management;

• Internet of things in a home area network (HAN) – home automation, comfort, energy management and energy efciency.

Internet of things for smart city

In the area of a smart city there are many potential applications of IoT technologies. In this article only few opportunities associated with energy management will be mentioned like energy efficiency and charging of electric cars and V2G-capable vehicles. They are:

• short and long term power supply planning, including construction of new network infrastructure and maintaining the existing one,
• energy management, in particular the reactive power compensation in summer when there is a high demand for reactive power due to the use of many air-conditioners,
• proper use of road lighting – for example, it can be dimmed after a certain time or depend on the amount of traffic,
• deployment of electric vehicle (EV) charging infrastructure in cities,
• emergency response applications – when a disaster (e.g. tornado, earthquake) hits an urban area.

Internet of things for smart metering

A key area in which there is a desired application of fog and IoT is an interface to the computing cloud/fog inside an energy meter, gas meter or a data concentrator. That ensures that the data billed by measurements would immediately be sent directly to the cloud computing and would be accessible from anywhere in the world for authorized users. In this case, it can be realised in two different ways:

• thanks to fog computing technology, where smart/gas/water meters are connected to border routers,
• thanks to cloud-based technology, where electricity and gas meters or data concentrators would send the data to the cloud via a suitable interface and software.

Adoption of this solution would drastically change the metering and billing devices system architecture as well as data processing capabilities and exploration of large data sets in an enterprise.

With this approach it would be possible to achieve added value. For example, smart energy meters or gas meters once an hour or even more frequently would send data to the fog. This could expose much more data than through the PLC technology which is characterized by a low bandwidth.

In case where such data would no longer be coming from energy meters located in a certain area, the fact would indicate existence of a network fault together with information about the area in which it occurs. On this basis it could be possible to indicate the potential network

element that is probably damaged and then properly equip and direct repair crews.

A very important problem is that gas meters do not have a guaranteed, fxed power supply, such as energy meters do. This strongly limits their communication capabilities including frequency of sending data to the cloud/fog computing. In such case the following solution can be taken into consideration: a gas meter sends data to an energy meter via communication technology with a low energy demand such as ZigBee and then the smart energy meter sends the data to the cloud computing.

Internet of things for transmission and distribution power grids

The currently proposed concept of smart power grids, there are many “dead spots”, where the monitoring could bring a lot of interesting information about the network infrastructure. Also there are many isolated islands of information, from which the exchange of such important information is sporadic, and their utilization – very small. Despite the fact that the degree of automation is improving, due to imperfections of information and poor ability to exchange information, many automated subsystems in electrical power system is fragmented, operating only locally and isolated, so they cannot provide a true and organic unity -a whole. So the level of the power grid intelligence as a whole is not high enough [5].

Advanced functionalities of smart power grid, which can be better achieved through the use of multiple sensors and advanced equipment supported by the Internet of Things technology by obtaining information from sensors located in the depth of the network, may be as follows.

1. Improved reliability of the power system - security of supply of electricity to customers:

• the ability to quickly repair itself (self-healing), in the event of any external or internal disturbances or threats; or even self-restoration of the network, after a failure, carry out dynamic reconfiguration to restore power after attacks, natural disasters, blackouts or failures of network elements; better diagnosis of the network, possible interference to the network such as wind acting on the overhead power lines, implementation of intended island operation,

• load shedding and system restoration that will allow the system operator to define groups of loads and allow the discharge of the load - lunching the following groups in order to ofoad the system in the event of having to take such an action. Of course, after the end of emergency state it will be possible to restore power to the disconnected load, which has been stripped of it. It will be possible to implement load shedding schemes: rotating, implemented in the round and linear. The amount of MW, of which you will need to reduce the load will be calculated automatically. Full power restoration can be done automatically or manually and will be maintained by the operator,

• the ability to create microgrids and autonomously powered islands in the event of a power failure. Better prediction of work conditions and level of power generated from renewable energy sources, by the use of atmospheric conditions sensors, combined with better

controllability of devices at customer sites, more devices, whose work can be adapted to the conditions of supply,

- damping of oscillations in the network, because the oscillation phenomena in the network should have a sufficiently low amplitude or be sufficiently suppressed, not to endanger the switching operations. Oscillations cannot persist for too long or cause to excite other remote generators that are not directly related to the cause of the oscillation network,

- use of automatic devices in place of different network connections such as cross-border links, which in the case of decrease in frequency or an overload or loss of synchronism occurrence interrupt the circuit at a particular location in the network. Such splitting points should be located in such areas that allow each of the isolated section of the network to balance production and consumption of energy in such a way that each section could continue to work in an acceptable range of frequencies and stability,

- coordinate the work of emergency automatics. Automatic failover can be used to prevent loss of stability of the group of generating units in unfavorable conditions,

- readjustment of excitation control systems. TSO should ensure that unit ARN (Automatic Voltage Regulators) settings and power system stabilizers in their regulation meet their requirements,

- quick units ofoading, which reduces the rapid mechanical energy transmitted by the turbine to the generator to improve the stability of the system,

- coordination of generating units work during network failures. TSOs control, in accordance with national grid codes, if the generating units meet the requirements of network fault tolerance when their stability is threatened. If a threat is detected during the stability calculations, the power systems can be equipped with adequate protection (causing disconnection of the power plant). In the event of loss of synchronism, the generating units are equipped with adequate protection equipment to disconnect them under certain conditions,

- voltage regulation in the power system, comprising of: automatic regulation of excitation and power generators voltage in power plants, regulation of transformers ratio under load conditions - automatic voltage regulation of the transformer is based on change of the position of the load tap through regulator in such a way that the voltage stays within the acceptable range of changes and by switching on and of the capacitor banks and the choke,

- changing the settings and coordination of power system protection automation to protect the electrical equipment in the event of damage occurrence, prevention of spreading of the failure and protection of people and equipment in the vicinity of damaged power system equipment.

2. Thanks to usage of a larger number of sensors and devices which can be controlled, some enhanced functions of SCADA (Supervisory Control and Data Acquisition) will be available - visualization, monitoring and control would apply to a larger number of elements:

- visualization showing sensitive situations occurring in the power system,
- through analyzes carried out in real time, performed online identifcation and visualization of the system work state: voltage and angular stability, and inventory stability, stabilization of the power system,
- the PMUs (Phasor Measurement Unit) will replace the previously used RTU (Remote Terminal Unit). SCADA system will detect the newly connected PMU device and will recognize it, will add to model of the system and it will start downloading data from it.

3. Management of power grid:

- energy savings by using voltage reduction – minimizing kWh consumption at the voltage closing to the lower end of the quality voltage 230V (± 10%), reducing the load while respecting the required voltage tolerance (during normal and emergency operation),
- improving the quality of energy supplied or in case of failure of supply of lower quality (not falling within the limits of quality) instead of complete stoppage of supply until the damage is repaired (it is necessary to design and manufacture equipment that would work properly, e.g. at a significantly reduced supply voltage - for example at source voltage equal to 150V instead of 230V, Some part of the devices could work properly, because they do need a lower voltage for working properly, such as 24V, 19V, 12V),
- minimizing line segments overloading,
- reducing or elimination of transmission lines overloading,
- to ensure reactive power supply for transmission or distribution nodes.

4. Renewable energy resources:

- better integration of distributed generation, wind speed and irradiance measurements, direction of clouds movement and temperature detection, etc.

5. Demand response:

- the use of advanced reaction of the DR (demand side response) in order to improve the ability to manage peak load,
- greater opportunities and better use of demand-side management, more sensors used at homes, more automated, intelligent household appliances, the ability to use automatic control of such devices, including the interruption to their work.

6. Interaction with end-customer:

- better interaction with energy end-users – the ability to create an interactive network connection in real time between users, power energy companies and energy equipment in

order to read the data in real time, fast, and bi-directional data exchange, which improve the overall performance of the integrated grid,

- better communication with customers, quick communication with the information from the sensors estimating failure time, and date of resumption of energy supply.

Often, the aim is to optimize the operation of the network by taking into account diferent purposes at diferent times, or by taking into account, in a balanced way, conficting objectives together.

Internet of things for asset management

There are evidences that it may be possible to use in a more optimal way the existing network assets. The optimal use of these assets may not be the goal, but only a mean to it.

Currently, the system may be missing data concerning the real system response to errors (e.g. fuses, reclosers, switches), the lack of such data hinders the ability to verify the effectiveness of past coordination. Improvements in the system coordination could improve its reliability [6].

Nowadays, the network operators work is „limited" because of the availability of only a portion of data on the state of the system for key assets (e.g., active power, reactive power, voltages, currents), and this limits the ability of operators to fully understand the present conditions (lack of situational awareness), analyzing problems and predicting the states in the future. Improvement of asset utilization depends on access to basic data needed to analyze and to take certain actions [6].

Currently, also the lack of integration between the various functionally related processes and technologies (e.g. management of disconnections, weather forecast, location and status of work crews, repair car problems, marking safety and technical drawings) affects the efficiency and efectiveness of distribution business [6].

There are several opportunities, related to resource / asset management which could be achieved or enhanced through use of Internet of things technology.

1. Monitoring the status and the operation of the assets:

- ubiquitous deployment of sensors which provide information about the status of work and "health" of all relevant assets,
- better management of assets, in particular, elements of the power grid, better diagnostics. Determining the status of individual network elements - allows precise electrical connection determination at the level of a single section of busbars,
- self-repair and reliable transmission of electricity – smart grids will be largely make use of advanced sensors, signal processing, information and communication technologies for monitoring in real time, the working conditions of transmission lines, transformers and circuit breakers. State monitoring system, based on distributed wireless sensors distributed in the

distribution network, in which are integrated intelligent modules with advanced signal processing and communication functions will measure constantly the key parameters of the line,

- measurement of cable sag, cable temperature determination, estimating the dynamic heat capacity, detection of vegetation near power lines, detecting line icing, galloping of power lines conductors (galloping cables is a dynamic effect caused by the impact of wind on the conductors of the power line), evaluation of poles mechanical strength, initial failure prediction of insulators or poles, identifcation of the critical limit of line capacity range, identifcation of line faults,
- clarifcation of assets issues before they cause further problems in the network,
- minimization of operation and maintenance costs, while increasing the working time of those assets,
- transformer state monitoring system will perform the analysis in real time, its proper operation, efciency, content of dissolved gases in oil, transformer taps changer load. On the basis of these parameters and working conditions of transmission equipment, it will be possible to detect, predict and respond to emerging problems before they will contribute to damage of the transformer (prevention) and not only in the situation after the failure, as it is happening nowadays,
- optimization of existing assets usage.

2. Maintenance:

- supporting of operational and maintenance works in order to clean the cables and remove ice, cleaning and lubrication of moving parts, which are opened and closed, e.g. dampers, switches, tightening and replacing screws, installation of sensors and measuring devices. Setting priorities: the ranking of equipment, grounds maintenance, preventive programs, intelligent hardware replacement programs, priority maintenance. Such analyses will reduce the probability of catastrophic failure, reduce maintenance costs and increase the reliability of the transmission system.

3. Planning:

- the ability to defer capital expenditures associated with purchase of new assets,
- on the basis of available knowledge better planning for both new and existing assets needed to meet the planned increase in the use of electricity, increase asset utilization state, improve the reliability of supply and new connections service.

Internet of things in substation automation

Functionalities of smart substation, which could be achieved or enhanced through the use of Internet of Things technology are as follows:

- autonomous control and adaptive security protection – in smart substations there will be used decentralized intelligent controllers with automatic power restoration. Settings of the

circuit breakers will be modified remotely in real time, in order to adapt them to changes in the network configuration [9];

• data management and visualization – all data obtained from the PMUs, transmitters, error recorders, electricity quality controllers etc. should be effectively managed and displayed [9]. Data visualization done in real time through the Internet of Things can give network operators a clear picture of the current state of the network;

• monitoring and alerting – information about changes of devices state or damage made to the equipment will be transferred immediately to the operator, e.g. in order to make them aware of possible risks, immediate warning alarm will be sent to mobile phones, pagers or through Intranet. For some devices, such as chargers, power supplies, UPS and fre alarm systems, signaling a fault occurs locally on the site. If the inspection of the station is not done for quite long time, the error may remain undetected for a long period of time. Ignoring some of these errors can cause a more catastrophic failure [9]. IoT will allow quick transfer of such information directly to the operator;

• diagnostics and forecasting – On-line status monitoring of the assets, based on advanced sensor technology ensures stable performance and reduces repair time. The expert system, based on error and faults identification technology will provide intelligent maintenance and management of devices in the station [9].

In the area of intelligent power stations IoT will be used for the following purposes:

• coordination – a smart substation through the IoT will be able to easily and quickly communicate and could be coordinated with other stations and surveillance centers. Protection system adaptation, in order to improve the security of the entire grid, should be achieved by coordination of surveillance centers.

• self-healing – a smart substation is able to dynamically reconfigure itself to pick up after the attacks, natural disasters, blackouts or partial network failures.

• restitution, that is restoration of power after a catastrophic failure.

Internet of things in micro-grids

One of the possible areas of application can be energy management in micro-networks, to balance the demand to the level of generation and energy storage capacity. Internet of Things will allow access to multiple sensors and enable fast transfer of data needed to microgrid controller, whose task will be ensuring a balance between energy generation and consumption.

Internet of things in a home area network

The Internet of things in the home area network will cover issues: energy efciency, home automation, convenience/comfort, energy management, charging of electric vehicle or V2G services, integration of renewable and distributed energy resources, smart meter, demand response: e.g. dynamic pricing, control of home appliances and thermostat.

When a person goes on a business trip, then home automation will reduce heating and cooling, turn of unnecessary lights to help the owner save on the energy bills. Presence sensors and motion sensors can control the lighting, blinds or curtains, temperature control.

The sensors (e.g. motion detectors) can be pet immune that means movement of pet animals will not cause the automatic function triggering [2].

Home automation can learn the habits of residents and adapt to them corresponding functions such as heating up a dinner when the children are returning from school. In addition to the smart refrigerators one can imagine smart dishwashers, washing machines, thermostats, lighting. Also sleep tracking beds, smart home locks, smart grill, which will guide a person through not burning food [2].

Table 1 The possible areas usage of different types of Internet of things technologies

Technology Area	smart objects	smart sensors	tags
Home area/smart buildings			
Energy efficiency	+	+	+
Convenience/Comfort	+	+	+
Home automation	+	+	
Energy management	+	+	+
Demand response	+	+	+
Electric vehicle	+	+	+
Renewable energy resource	+	+	
Smart meter	+	+	
Micro-grid	+	+	+
Outage detection	+	+	
Power grid			
Self-healing	+	+	
Monitoring the state of transmission lines	+	+	
Monitoring the state of distribution lines	+	+	
Voltage and var control	+	+	
Substation automation	+	+	
Power system protection	+	+	
Controlling and monitoring the power grid	+	+	
Monitoring the status of power grid elements e.g. breaker, recloser			
Controlling dispersed RES power plants	+	+	
Restoration of power	+	+	
Operating in grid/islanded mode	+	+	
Balancing between generation and consumption	+	+	
Cyber security	+		
Asset management	+	+	
Monitoring the state of power grid elements e.g. breaker, transformer	+	+	
Smart city (only energy areas)			
Energy management	+	+	
City vehicle/ City Car	+	+	+
EVs infrastructure	+	+	
Emergency response applications	+	+	+

Source: own evaluation.

Conclusions

The use of the Internet of Things will improve the existing possibility that monitor and control of the power grids. There will come up new opportunities and new technologies. The Internet of things with fog or cloud computing can be used in many areas of the intelligent power network. Therefore, these technologies should be regarded as highly prospective.

This will increase the level of power system digital safety risk. Much more information is a greater risk of distortion of any of them. Uncertain data is a risk of distortion of physical processes in controlling of the power system operation.

Much larger number of sensors and power electrical devices makes a higher risk of power system disorder, due to damage to the system in one of these devices. Managing huge amounts of incoming data makes necessary to use very complex algorithms. It is all a kind of price for the availability of additional information.

REFERENCES

[1] Brejecka, K., *Will Linux enable to standardize the Internet of Things*, Computerworld, 24.04.2014.

[2] Duncan G., *You can't avoid the 'Internet of things' hype, so you might as well understand*, Digital Trends, 24 January 2014, http:// www.digitaltrends.com/home/heck-internet-things-dont-yet/

[3] Jablonska M., *Internet of things in smart grid deployment*, Rynek Energii, 2(111)/2014.

[4] Ling Zheng, Shuangbao Chen, Shuyue Xiang, Yanxiang Hu, *Research of Architecture and Application of Internet of Things for Smart Grid*, International Conference on Computer Science & Service System (CSSS), 2012, Issue Date: 11-13 Aug.

[5] Miao Yun, Bu Yuxin, *Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid*, International Conference on Advances in Energy Engineering (ICAEE), 2010.

[6] National Energy Technology Laboratory, *Electric Power System Asset Optimization* DOE/NETL-430/061110, 07.03.2011.

[7] *UCTE-OH – Temat 3: Bezpieczeństwo ruchowe* (ostateczna wersja 1.3 E, 20.07.2004).

[8] URE, *Koncepcja dotycząca modelu rynku opomiarowania w Polsce, ze szczególnym uwzględnieniem wymagań wobec Opera-tora Informacji Pomiarowej*, Portal URE, Warszawa, 09.05.2012.

[9] Zhenhua Jiang, Fangxing Li, Wei Qiao, Hongbin Sun, Hui Wan, Jianhui Wang, Yan Xia, Zhao Xu, Pei Zhang, *A vision of smart transmission grids*, Power & Energy Society General Meeting, 2009. PES '09. IEEE, 2009.

[10] Jiang Zhu, Chan D.S., Prabhu M.S., Natarajan P., Hao Hu, Bo-nomi F., *Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture*, IEEE 7th International Symposium on Service Oriented System Engineering (SOSE), 2013, Issue Date: 25-28 March 2013.

[11] *Fog Computing, Ecosystem, Architecture and Applications*, Cisco, Project ID: RFP-2013-078.

[12] Madsen H., Albeanu G., Burtschy B., Popentiu-Vladicescu F.L., *Reliability in the utility computing era: Towards reliable Fog computing*, 20th International Conference on Systems, Signals and Image Processing (IWSSIP), 2013, Issue Date: 7-9 July 2013.