Smart technology, overview, and regulatory framework

Marian ION[1,2], **George CĂRUȚAȘU**[1, 3]
[1]Doctoral School, University Politehnica of Timișoara,
[2]National Institute for Research and Development in Informatics,
[3]Department of Informatics, Statistics and Mathematics, Romanian-American University
ionmarian@gmail.com, carutasu.george@profesor.rau.ro

Abstract: Smart systems are already part of our lives. Modern technologies entered our lives with the first industrial revolution, when machines first began helping or replacing humans in work. This was followed by the needs of communities to improve the life of people in common tasks such as lighting, street cleaning, garbage collection and processing, water management, energy management, etc. Lastly, as the technology developed and, eventually, became more and more miniaturized and improved, the needs of individuals joined. While, at the beginning of the process, risks were more physical and related to technology reliability, we are facing new challenges that need to be tackled on multiple layers, from regulatory perspectives, to energy safety, personal security, to usage of personal data or remote alteration of equipment. Currently technologies know more about our lives, needs, habits, than ever before and we, as individuals and communities, must ensure a safe use of these systems for people literate or illiterate in state of the art technologies or cybersecurity. Therefore, the article will provide a brief technological insight to smart systems, as well as a brief overview to the European Union regulatory framework and initiatives on smart systems and technologies.

Keywords: smart system, smart technology, regulatory framework, cybersecurity

INTRODUCTION

As social beings we tended, during history, to gather ourselves in communities made of people with common purposes and activities in their existence. Some of these purposes relate to the safety of a person or his group, to food and survival, to energy or transportation means, to human interaction or common actions in order to ensure growth and development as individuals, or communities. In time communities grew increasingly larger, reaching out to present populations that were found in an entire country a thousand years ago.

Progressively, part of the purposes motivating a person to join a community evolved, refined, but few remained constant in human history. Thus, primary motivations that led to building human communities are still there today in the individual and collective mental, even if at a subconscious level, and are still related to personal and group safety, survival, to energy provision and means of transportation, to human interaction and common activities and interests.

The accelerated development of human communities of the last hundreds of years led to the need to solve some critical aspects on public health, fresh water provision, access to sewage systems, energy and fuel provision, gathering, deposit and processing of wastes, access to means of transportation and education for continuously growing numbers of people, covering continuously growing horizontal and vertical areas. The accelerated technical evolution started with the industrial revolution led to the identification of new technical ways to solve the identified needs, culminating in the last decades with the smart technologies generated by the digital and microelectronic revolutions. Obviously, the technological development will continue to shape the human society as a whole or communities, as well as every individual person, depending on the exposure and tolerance of each of them.

Currently cities sum up more than 50% of the globe population, and the problems with the infrastructure, public health and the environment they face, are very similar. The technological means available represent the only way cities and metropolitan areas, or large human communities, will be able to solve these problems. In this perspective all important cities and metropolitan areas, as well as some medium size communities, implement or already implemented a series of technologies to facilitate the provision of public services and utilities to their inhabitants. Gradually, the technology will get to serve all human communities, independent of their sizes. Thus, the technological revolutions, and we need to highlight here the computer and the electronic communication revolutions, made possible the large scale automation of equipment and installations serving infrastructure public services in cities and other localities with large human communities. In this perspective, gathering and processing useful data, along with data transmission in machine-2-machine intelligible language, represent the fundamental elements to use smart technologies at residential, business or community levels. Data gathering, the transmission and processing of data for decision making, represent also main technological processes carried-out automatically and on permanent basis with respect to the commands given by automatic control systems or designated human operators.

As a language convention, we will continue to use the term “smart technologies” to encompass all digital control technologies for domestic equipment (e.g. smart home, smart household appliances, etc.), personal (e.g. wearables), medical, industrial (e.g. SCADA – Supervisory Control and Data Acquisition, IIoT – Industrial Internet of Things, etc.) or dedicated to public services (e.g. smart city, smart community, etc.), connected to Internet or other data networks, and remotely controlled by specialized or general use hardware or software systems.

With regards to all above, we may consider a smart technologies system is an aggregation of integrated technologies with the purpose of large scale automation of processes meant to monitor and control environments or external systems made to improve human life and work, or to increase the productivity of industrial or repetitive activities. From this perspective, the most visible applications are in automatic production systems, and smart city systems. As more and more technologies become available to the public, the number and severity of associated risks raise, and need to be managed on large scale on technical aspects (e.g. vulnerabilities management, device hardening, standardization, interoperability), as well as awareness and legislation. Therefore, the article presents an overview on current technologies, lists applicable legislation (EU and national level), as identifies some of the relevant initiatives taken to manage identifiable and predictable cybersecurity risks on smart technologies.

OVERVIEW OF SMART TECHNOLOGIES

The origin of modern industrial control system lies in the 1960s, when process control was applied with electrical systems. SCADA originates in the 1970s and is dedicated to large scale monitor and control of critical or industrial processes, similar to the Distributed Control Systems (DCS) used to control delimited areas like a factory, refinery, etc., but on a smaller scale and few minuses than SCADA. Meanwhile, IoT (Internet of Things) technologies belong to new technological waves of the last years, Industry 4.0, and developed on market segments complementary to SCADA systems, like vehicle control, smart households, smart city, etc. joining together control systems and the Internet on a larger scale. From a larger list, SCADA and the more recent Internet of Things (IoT) technologies became the most relevant. Considering the large variety of IoT technologies, we should mention, though, that IIoT is more relevant in the context of the article. However, they resemble each other in functionalities and technological aspects, and some public opinions consider the transformation and modernization of SCADA systems as a convergence to Industry 4.0.

Different ways are used to represent ICS (Industrial Control System) architectures. In a classical approach a smart system, such as SCADA, is typically considered in a 3-tier architecture: the field devices layer (inputs and commands), the control/processing layer, and the supervision/management layer. An example of this representation of a 3-tier SCADA architecture was published in 2010 by IEEE (Institute of Electrical and Electronics Engineers):

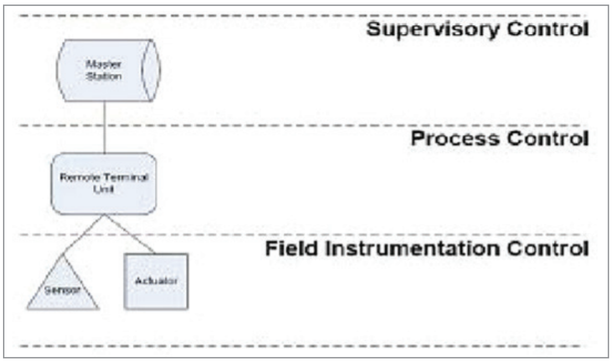

Fig. 1: *IEEE 3-layer SCADA system architecture [IEEE 2nd ICAE, 2010]*

IEEE presents itself as "an association dedicated to advancing innovation and technological excellence for the benefit of humanity, is the world's largest technical professional society." (https://www.ieee.org).

The lowest layer is the field layer, containing field devices meant to collect data and control parameters of the target system or environment. Devices that may be found in this layer are sensors to collect environmental data (temperature, pressure, heat, etc.), actuators to convert command signals to movement (pumps, valves, articulations, motors, etc.), relays to transmit electric signals to selected actuators or equipment, etc. Collected data is sent "upward" to the middle layer for processing using specific data communication links. Similarly, commands are commonly transmitted using the same main communication links but in the opposite sense.

The control/ processing layer receives collected data from the field layer or command data from the upper layer, and contains equipment and software programs to process the data it received, and forward the result to the destination layer. After processing, collected data is forwarded to the upper layer to be presented to operators, while command/control data is forwarded to the field layer to be executed by the devices. Equipment like RTUs (Remote Terminal Unit), PLCs (Programmable Logic Controllers) or IEDs (Intelligent Electronic Device) are found in the processing layer.

The upper level contains analysis and reporting equipment and software application (e.g. MTU (Master Terminal Unit), HMI (Human Machine Interface) on SCADA systems, dashboards, analytic, etc). The presentation of data is usually designed for human operators, whether they take actions manually, or not. In many cases the layer may contain elements to automatically perform calculations based on predefined parameters and transmit commands to be executed in the field layer with, or without human supervision or intervention.

In different representations, the processing and supervision components are considered distinct layers, while in others are regarded as a single layer, the differentiation coming from the field devices (inputs layer / commands layer). An example of this approach is presented by the International Society of Automation (ISA):

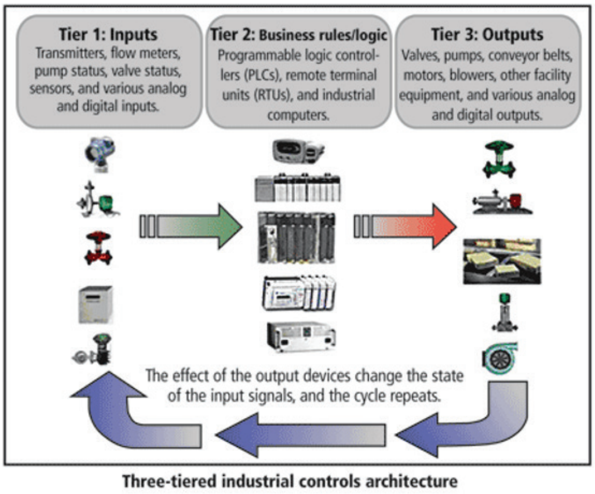
Tier 1: Inputs
Transmitters, flow meters, pump status, valve status, sensors, and various analog and digital inputs.
Tier 2: Business rules/logic
Programmable logic controllers (PLCs), remote terminal units (RTUs), and industrial computers.
Tier 3: Outputs
Valves, pumps, conveyor belts, motors, blowers, other facility equipment, and various analog and digital outputs.
The effect of the output devices change the state of the input signals, and the cycle repeats.
Three-tiered industrial controls architecture

Fig. 2: *ISA 3 layer SCADA system architecture [ISA, 2005]*

The International Society of Automation is a global, nonprofit organization with more than 40,000 members worldwide, working closely with ANSI (American National Standards Institute) in developing international standards applicable to SCADA systems and batch process control.

As already mentioned, a smart system cannot function properly, without data links. The communication layer may be regarded as a vertical layer connecting all 3 layers and facilitating the interaction between them, as well as between elements in the same layer:

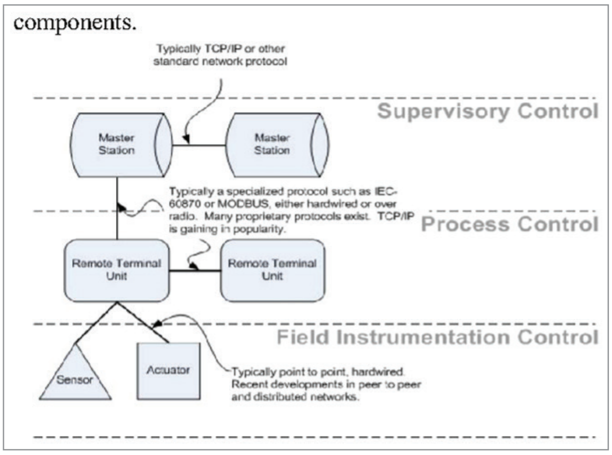
components.
Typically TCP/IP or other standard network protocol
Supervisory Control
Master Station
Master Station
Typically a specialized protocol such as IEC-60870 or MODBUS, either hardwired or over radio. Many proprietary protocols exist. TCP/IP is gaining in popularity.
Process Control
Remote Terminal Unit
Remote Terminal Unit
Field Instrumentation Control
Sensor
Actuator
Typically point to point, hardwired. Recent developments in peer to peer and distributed networks.

Fig. 3: *IEEE Data communication between architecture layers [IEEE 2nd ICAE, 2010]*

Data is transmitted between layers based on standardized protocols, considering the level of the communication. For example, considering that field devices are commonly low power devices in order to reduce energy consumption, and data is transmitted in very small packages, specific protocols may be used such as: ProfiBus, FieldBus, HART, etc. Data between the middle and the upper layers is strongly migrating to Ethernet standards and the TCP/IP protocol stack from protocols like ModBus, or DNP3. It is important to reiterate that the communication layer is mandatory for a smart system to function properly. The more recent IoT brings standardization to a new level, using several protocols running on top of the TCP/IP stack for data transmission.

With regard to the newer IoT, considering the significant diversity of "things" and available technologies, there is no common view on the architecture yet, there is no generally accepted topological or technical standardization. Still, things are moving in this direction, the industry and responsible bodies are working together towards standardization in order to stimulate market development. Also, quite similarly to SCADA, an IoT architecture is commonly viewed in a 3 topological layers, one related to the physical devices layer, one to the network level, and one to the application layer.

In 2012, in an attempt to standardization ITU (International Telecommunication Union) proposed a 4 layers reference model for IoT architectures *[Recommendation ITU-T Y.2060]*, containing the application layer, the service support and application support layer, the network layer, and the device layer, as well as 2 vertical layers on security and management capabilities:

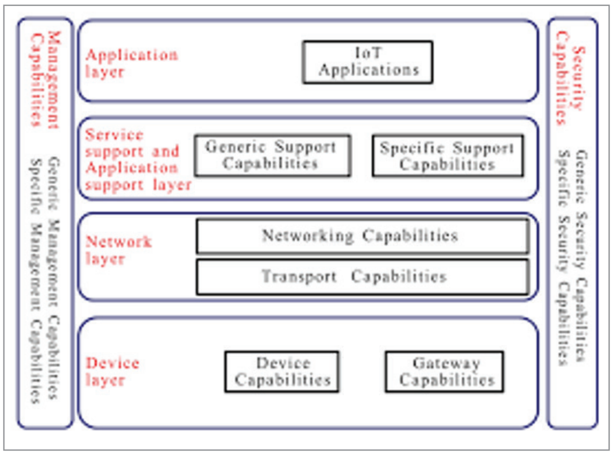
Management Capabilities
Generic Management Capabilities
Specific Management Capabilities
Application layer
IoT Applications
Service support and Application support layer
Generic Support Capabilities
Specific Support Capabilities
Network layer
Networking Capabilities
Transport Capabilities
Device layer
Device Capabilities
Gateway Capabilities
Security Capabilities
Generic Security Capabilities
Specific Security Capabilities

Fig. 4: *ITU IoT architectural model [ITU, 2012]*

However, as can be seen from ITU's reference model, work needs to be done furthermore to switch from top level reference models, to more technical ones. Considering these, despite some proposed models, a smart system is now more than a simple measurement and control system. In addition to physical elements specific to field measurements and actuators, as well as management components, the system contains significant amounts of hardware, software, storage, networking, and cybersecurity technologies making it very similar to ICT (Information and Communication Technology) systems. Therefore, from a more detailed architectural perspective specific to complex informatics systems, we propose a more applied, a more balanced approach of a smart integrated system, considering the following basic components:

- physical layer, containing the data collection and command and control sub-systems;
- electronic communication layer, containing the data transformation and data transmission sub-systems;
- data storage layer, containing the data storage and data archiving sub-systems;
- data processing layer, containing data processing and data presentation sub-systems.

Similar to ITU's comprehensive model, 2 supplementary vertical layers should be added, with security and management/administration capabilities. While one of these layers deals with cybersecurity aspects on all the others, the other handles the infrastructure's managing functionalities.

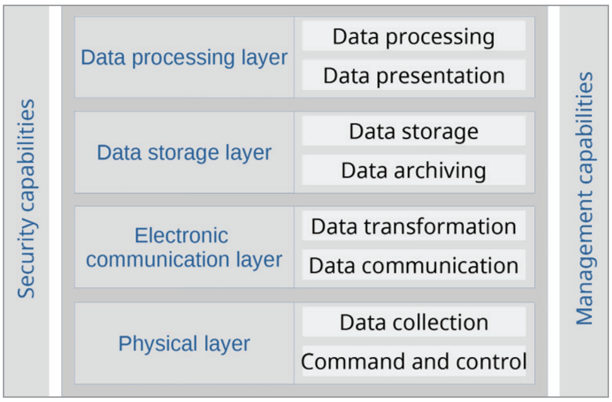

Fig. 5: *Proposed model of smart system architecture*

As it may be seen, the proposed architecture differentiates the classic models, bridging the 2 domains and emphasizing in proper measures both, the ICT components and the elements specific to ICS systems. A smart system contains, in relatively equal proportion, ICS and ICT technologies, and we think any perspective on modern smart systems should consider both. Moreover, as technology evolve moving from "smart" to "intelligent" systems, the ICT component will become of higher importance, artificial intelligence being a good example of one of the game changing technologies. Despite the fact that modern artificial intelligence initiated in the 1950s, with some step-backs in the second halves of the 1970s and the 1980s, only from the 2000s we are witnessing a very strong revival of the domain, with current applications on all areas, including industrial processes, smart city, data processing, etc.

Implicitly, considering the new model, the basic functionalities of a smart technologies integrated system follow the proposed n-tier architecture representation, and are as follows:

- data collection/gathering, at the data collection layer;
- data transformation (analog to digital, digital to digital) and data transmission, through the electronic communication layer;
- data preservation in active storage and digital archive, at the data storage layer;
- data processing, data presentation and reporting in human readable, decision making at the processing layer;
- decision transmission through the electronic communication sub-system;
- decision application through the command and control sub-system in the physical layer;
- alert, report, notification of human operators through the processing and reporting sub-system.

The data collection sub-system is made of multiple sensors and data concentrators. Sensors may be analogue or digital, as well as the data they collect. Usually, until reaching the data processing and reporting sub-system, if needed data passes through a process of transformation from an analogue to a digital format using an ADC equipment (analogue to digital converter) that will sample the analogue signal at a predefined time rate, and will retain and further transmit the sampled values. Data collected from the beginning in a digital format will eventually pass through a transformation process (digital to digital) in order to apply specific algorithms or transformations on the data. Data processing in modern systems based on smart technologies will always be digital. While a residential system may contain several dozens smart devices, an industrial or smart city system may contain tens of thousands or more, sensors and actuators of different types and categories. The data collection component is designed to permanently, repeatedly at specifically defined time frames, collect data relevant for the proper functioning of the smart system, as well as the target environment or system. Therefore, from a general view, collected data fits in one of two great categories:

- data about the relevant parameters on the target environment or system;
- data about the relevant parameters on the smart system.

Data on the target environment or system describe, through their collected correlated values, the current status of the target and the result of the actions performed by the smart system. Monitored parameters cover a very wide range, from environmental parameters (e.g. temperature, light, humidity, air quality, soil quality, rain, wind strength, etc.) to human made systems (e.g. public lighting system, public transportation system, public parking system, smart appliances, smart house, etc).

Data on the smart system describe, through their collected correlated values, the operational status of the technological system as a whole, as well as in components. That way, monitored system parameters cover the operational status of the component layers such as: data collection (e.g. sensors, signal concentrators, remote terminal units, actuators, etc.), electronic communication (e.g. ADC, DDC, DAC, GSM, WiFi, NBIoT, data modems, routers, switches, etc.), data processing layer (e.g. hardware servers, CMS processing stations, software components and applications, etc.), data storage layer (e.g. SAN, NAS, servers, tape backup equipment, optical backup equipment, etc.).

The electronic communication layer is responsible with the transformation and transportation of data from the sensors or signal concentrators to the elements of processing and reporting layer as well as back, from them to elements of command and control installed in the target environment or system. Layer's sub-systems are made of specialized electronic communication equipment (e.g. AD converters, DA converters, DD converters, GSM modem, WiFi router, NBIoT equipment, WAN router, LAN switches, etc.) and the transmission medium itself that may be wired (data cable, FO, electric cables, power lines, etc.) or wireless (radio spectrum for civil applications on long distances, unregulated radio spectrum for civil short distance communication, WiFi, GSM 3G, 4G, 5G, IoT narrow band, etc.). It should be pointed out that the data communication sub-system includes the data transmission from the target environment or system to the central system (sensors → central system), the data transmission from the central system to command & control elements installed on the target environment or system (central system → actuators), as well as internal data transmission between functional or technical components of the central system (e.g. application servers, databases servers, switches, firewalls, routers, storage, electronic archive, etc.).

The layer for data processing and presentation contains a number of servers (hardware components) and dedicated applications (software components) processing data from the data collection sub-system through the electronic communication sub-system, as well as presenting them to the operators in a human readable form. In this context, data processing means the process where data is transformed, applied in algorithms, interpreted and correlated, in order to gain meaning for the human operator. Considering the technology (e.g. SCADA, DCS, IoT, IIoT, etc.), data processing may be performed in dedicated servers with dedicated software applications, as well as in general purpose servers allocated to data processing using dedicated software applications. Thus, data processing is always done in dedicated software applications, only the physical infrastructure (servers) varying dependent of technology. Therefore, data processing consists in data transformation or normalization to necessary types or formats, application of specific algorithms considering the scope of processing, correlation of results and the use of them in analyses and decision processes on the external, target environments' or systems' management.

The data processing layer includes also visual interfaces such as HMI (Human-Machine Interface), dashboards, Graphical User Interface

(GUI), etc., meant to present human operators, in intelligible form, correlated or uncorrelated data like: lists, graphics, maps, tables, alerts, etc. Data presentation may also be performed by other means like: predefined or custom reports, alerts raised on predetermined conditions of time (planned reports or notifications), objective (reports or notifications on fulfillment of certain activity conditions), or risk (reports or notifications on certain situations or risk conditions regarding the target environment or system, or the smart system itself), etc. The sub-system also includes management interfaces whose purpose is to facilitate the administration of the system, component elements, or system security, as well as means to utilize or present data to external systems or human operators.

Data prone to processing, as well as data and information resulted from processing, will be stored and kept in the storage and archiving sub-system. The storage and archiving sub-system consist in a series of equipment and dedicated software applications designed to save and preserve data on short to long term. The technologies falling in this category may be:

- databases, consisting on database equipment (dedicated or general purpose servers) and DBMS / RDBMS software applications;
- Dedicated network storage equipment (e.g. SAN, NAS, other server-based solutions);
- Cloud-based storage;
- Dedicated long term storage equipment (e.g. tape storage, optic disks storage, etc.).

Databases may contain active data, recent (precedent) data, and historical data, necessary to fulfill the purpose of the informatics system, along with other complementary data necessary for system functioning or data processing. Data in databases may be stored in a normalized or un-normalized, non-standardized form, requiring eventual transformations before processing. It is important to specify that data in smart systems is always structured, making it easier to store and manipulate data in SQL Databases (DBMSs / RDBMSs), instead of new trends such as Non-SQL Databases. Storage equipment is intended to facilitate data and document saving for current or future usage, as well as in archiving purposes. Short term storage process is intended for current or recent data, with a higher probability to reuse or report. Medium/long term storage is intended for data not used in current processes, but not necessarily reaching the archiving conditions. The archiving process, instead, is for historic data with limited potential to reuse or report, but need to be kept for historical or eventual usage purposes. The archiving procedure is applied periodically, automatically or user triggered (manual process).

Following data processing, the smart system will try to apply the taken decision based on automatic or human-based means, on the target environment or system. The command and control sub-system is responsible with the application of these decisions. The decisions represents, actually, commands that will be applied to control equipment, having as result controlled modifications of some parameters of the target environment or system. Simple examples are starting a lightning system at sunset, starting a backup power system when the electric energy grid becomes unavailable, starting an irrigation system due to drought conditions, etc. Commands are either analog (e.g.: electrical, electromechanical, magnetic, electromagnetic) or digital, and are transmitted to command elements such as PLC/RTU, process computers, relays, etc. Commands transmission is made through the electronic communication sub-system.

Checking and adjusting the results of the applied commands is done by reiterating this cycle, from collecting data from the target environment or system, to analyzing it, adopting new decisions and applying them to the target. Aligned with the fact that all environments or systems are basically open systems, subjects to exterior influences, the ensemble of target environment or system, and the smart technologies control system may also be regarded as an open system, functioning in feedback loops by continuously, repeatedly performing actions like: monitoring the target environment or system, controlling its key parameters and adapting measures to ensure stability and consistency of the it.

EUROPEAN UNION REGULATORY ASPECTS ON SMART TECHNOLOGIES AND SYSTEMS

The role of this section is to present an activity summary of communautaire bodies in the implementation and development of smart technologies at European Union level, as well as aspects related to standardization, interoperability and security of equipment or data. The section represents a presentation of relevant EU documents and actions related to the above-mentioned subjects, with no intention to represent an exhaustive screening of regulations and other relevant documents and actions.

Smart technologies are not strictly regulated at European Union level, in other aspects than electronic compatibility or the interdiction to use military radio frequencies. Also, few technological standards were issued by European standardization bodies. At European Union level was, however, generated a common vision on aspects related to smart technologies and systems through a series of actions undertaken mainly during the last 20 years by the European Commission and other responsible bodies *[European Commission, The Internet of Things]*. The first actions in the European Union started in the early 2000 and were related to recognizing the importance of critical infrastructures to the well-functioning of the modern human society. The European Council in June 2004 requested the preparation of a strategy to protect the critical infrastructures. In October 2004 a "Communication on Critical Infrastructure Protection in the Fight against Terrorism" *[COM/2004/0702 final]* was published by the Commission, raising issues on prevention, readiness and response to terrorist attacks on critical infrastructure. In December 2006 a Communication from the Commission on a European Programme for Critical Infrastructure Protection *[EPCIP, COM/2006/786 final]* was published, with the general objective of EPCIP "to improve the protection of critical infrastructures in the EU … by the creation of an EU framework concerning the protection of critical infrastructures …". The Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection establishes, as it clearly mentions, "a procedure for the identification and designation of European critical infrastructures ('ECIs'), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people". The directive became the central point in the implementation of the European Programme for Critical Infrastructure Protection.

Several regulations, communications, reports and studies issued at EU level on different subjects are also referring smart technologies and smart Control Systems (e.g. SCADA, DCS, IoT) from perspectives of market growth, standardization and interoperability, resilience or cybersecurity (European Union legislation portal).

The Communication from the Commission: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience (COM/2009/149)" *[European Commission, 2009, on COM/2009/149]*. As the communication clearly specifies, it recognizes critical information systems as vital for EU economy and growth, and "focuses on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs" (Critical Information Infrastructures).

The Communication from the Commission: "A Digital Agenda for Europe (COM/2010/245)" of 2010 *[European Commission, 2010, DAE]*, with the purpose to "to deliver sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and inter-operable applications." The Digital Agenda defines the enabling role of ICT in EU's smart and sustainable growth, including the role of smart technologies.

The Digital Single Market Strategy (COM/2015/0192) adopted in May 2015 *[European Commission, 2015, DSMS]*, contains elements to accelerate the development of IoT and promoting electronic interoperability.

The working document "Advancing the Internet of Things in Europe" published in April 2016 *[European Commission, 2016, SWD(2016)110]* is part of the initiative "Digitising European

Industry” *[European Commission, Digitizing European Industry]*, and the identification of 3 pillars standing at the base of the European Union vision on IoT, respectively:

- “a thriving IoT ecosystem”;
- “a human-centered IoT approach”;
- “a single market for IoT”.

The Communication from the Commission “ICT Standardization Priorities for the Digital Single Market (COM/2016/176)” *[European Commission, 2016, ICT Standardization]* brings to attention the role of standardization and interoperability in the Digital Single Market, and proposes the adoption of a “Trusted IoT label” and a certification scheme for this.

The initiative “Building a European data economy” of January 2017 *[European Commission, 2017, European Strategy for Data]* is part of the strategy on single digital market, facilitating the growth of the digital economy in the benefit of the society and the European economy by promoting data reuse and free circulation within the common market.

The Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 *[European Union, 2017, Regulation (EU) 2017/1938]* deals with measures to safeguard the security of gas supply, including risks related to cybersecurity and ICT reliability.

Commission Regulation (EU) 2017/1485 of 2 August 2017 *[European Commission, 2017, guideline on electricity transmission system operation]* establishes a guideline on electricity transmission system operation and includes provisions related to data exchange and cybersecurity risks.

Commission Staff Working Document “Liability for emerging digital technologies” *[European Commission, 2018, SWD(2018)137]* accompanying the document “Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe” *[COM(2018) 237 final]*. The April 2018 working document deals with subjects related to products safety and legal accountability on emerging digital technologies, including IoT.

Commission Implementing Decision (EU) 2018/637 of 20 April 2018 *[European Commission, 2018, 900 MHz and 1800 MHz standardization]* amends Decision 2009/766/EC on the harmonization of the 900 MHz and 1 800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community as regards relevant technical conditions for the Internet of Things.

Commission Staff Working Document “Impact Assessment” Accompanying the document “Proposal for a Regulation of the European Parliament and of the Council on ENISA”, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (‘’Cybersecurity Act’’) *[European Commission, 2017, SWD(2017)500]* provides an insight on ENISA activity since its establishment and emphasizes some of the aspects that became relevant concerning cybersecurity, public awareness and necessary measures.

The June 2019 study “Mapping Internet of Things innovation clusters in Europe” by the Internet of Things (Unit E.4) from the European Commission *[European Commission Unit E.4, 2019, IoT Innovation Clusters]*. The study provides, as it clearly states, “an extensive analysis of the European ecosystem, within which IoT solutions and applications are developed. It describes and assesses the processes and dynamics of IoT clusters, their key drivers, and sustainability and key success factors”. Areas of interest targeted by the study were: smart living, smart farming, wearables, smart city, smart mobility, smart environment and smart manufacturing. Unit E.4 Internet of Things *[European Commission, Unit E.4]* is one of the competence center of the European Commission in IoT, and is responsible with drafting policies, studies, standards, new business models supported by IoT technologies to increase the competitivity of European industry.

In March 2015 the European Commission initiated the establishment of the “Alliance for Internet of Things Innovation”(AIOTI), as not for profit organization, having at current time over 160 members, from the market (technological and consultancy companies), standardization bodies and research institutes from within or outside the EU. The organization has the scope to raise the degree and adoption speed on IoT technologies in the Union. The objectives considered, as comes out of the Alliance's web-site, (www.aioti.eu), are: strengthening the dialog and interaction between actors into the European market of smart things, increasing standardization and interoperability, promoting research and development in IoT.

AIOTI represents the most comprehensive initiative in the field of smart technologies in Europe, with the activity organized in 13 working groups covering a very wide range of elements, such as: policy, research, standardization, smart living for age well, smart farming, smart cities, smart mobility, smart utilities, smart manufacturing, smart buildings, etc. In January 2017 AIOTI published an important document, "Report on Workshop on Security & Privacy in IoT" *[AIOTI, 2017]*, following a workshop hosted by the European Commission. The report emphasized the conclusions of the workshop and identified a series of minimum baselines on security and privacy requirements on wearable equipment, autonomous vehicles, personal data and privacy, IIoT security, and smart city.

ENISA (European Network and Information Security Agency), the European agency for cybersecurity established by the European Commission in 2004, maintained in time a considerable effort to regulate and issue guides and recommendations on the smart technologies domain. In this aspect, the following relevant documents worth mentioned (ENISA).

- "Protecting Industrial Control Systems. Recommendations for Europe and Member States" of December 2011 *[ENISA, 2011]*. The study emphasizes on several actions that operators of ICS (Industrial Control System) technologies should take. The recommendations are also important for operators of critical infrastructures, as all of them are managed using some type of ICSs.
- The "Good Practices for an EU ICS Testing Coordination Capability" Report of December 2013 *[ENISA, 2013]*, analyzes the current status in ICS security testing capabilities and "tries to identify existing resources and foreseen challenges in order to enable unified and consistent ICS security testing capabilities to be created across Europe" in a harmonized, independent and trustworthy manner.
- In the "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" Report *[ENISA, 2017]*, November 2017, ENISA defines a common set of baseline security recommendations for IoT systems, with the purpose to "provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems" and the issuance of a set of 7 general recommendations to be followed by operators of critical infrastructures.
- The report "Towards secure convergence of Cloud and IoT" of September 2018 *[ENISA, 2018, Convergence of Cloud and IoT]*, analyzes a number of cybersecurity issues regarding cloud computing and Internet of Things infrastructures, proposing a series of guidelines that can be applied to increase the level of cybersecurity by preventing problems and remedying those identified.
- "Introduction to IoT security" *[ENISA, 2018, Forth NIS Summer School 2018]*. ENISA has organized specialized training on IoT technologies and has published training materials, such as the summer school 2018 on cyber security of IoT technologies. The organized course reflects the activity of ENISA in the field of Internet of Things technologies, presents in detail the vision of the Agency on the important aspects for the security of the smart technologies at sectoral level and presents a series of specific case studies.
- "Good Practices for Security of Internet of Things in the context of Smart Manufacturing" of November 2018 *[ENISA, 2018, Good Practice IoT]*. In this study ENISA collected a set of good practices to increase the security of IoT systems in the context of the Industry 4.0 / Smart Manufacturing revolution. The study also aims to standardize

relevant terminology and taxonomies, map threats to assets and propose some security measures to be taken against the threats.

- "IoT Security Standards Gap Analysis Mapping of existing standards against requirements on security and privacy in the area of IoT" v. 1.0 of December 2018 *[ENISA, 2018, Gap Analysis]*. Te overall goal of the study for ENISA is to "map requirements on security and privacy in the area of IoT to existing standards, identifying the gaps".
- "Industry 4.0 Cybersecurity: Challenges & Recommendations" of May 2019 *[ENISA, 2019]*. The document is the result of a gap analyzes performed by ENISA to identify the main challenges in implementing security measures for Industry 4.0 and IIoT, based on 3 categories: people, processes, and technologies.

Following the entering into force of the Cybersecurity Act *[European Union, 2019, Regulation (EU) 2019/881]*, ENISA is currently working to prepare "European cybersecurity certification schemes" as basis for the certification of products, processes and services that support the delivery of the Digital Single Market, including smart technologies.

BEREC (Body of European Regulators for Electronic Communication) is another European body established to facilitate the consistent application of EU regulatory framework in the telecom sector and an effective internal sectorial market. BEREC was established in 2009 as part of the Telecom Reform Package *[European Union, 2009, Regulation (EC) 1211/2009]*. The initial regulation was superseded in 2018 by Regulation (EU) 2018/1971 of the European Parliament and of the Council *[European Union, 2018, Regulation (EU) 2018/1971]*. As well, the Telecom Reform Package or 2009 was replaced by the Directive (EU) 2018/1972 of the European Parliament and of the Council *[European Union, 2018, Directive (EU) 2018/1972]*. The directive establishes the European Electronic Communications Code, as well as new responsibilities for BEREC, such as: issuing guidelines on relevant topics, technical reporting, implementing sectorial databases, matching opinions on subjects related to the internal market, etc.

In the last years BEREC, the Body of European Regulators for Electronic Communication, following public consultations, published a series of documents regarding smart technologies, such as:

- The report "Enabling the Internet of Things" (BEREC, 2016), 2016, considering the description of the technology, its functionalities and characteristics. Also, the report analyzed the need for new regulation considering the potential impact on the society and human life.
- The report "Internet of Things indicators" *[BEREC, 2019]*, 2019. The report aims to assess "what type of measurement of IoT NRAs are already conducting on the supply-side, and assesses if there is, at this stage, any common set of IoT-related indicators which BEREC or National Regulatory Authorities ('NRA') could regularly collect in the coming years (possibly from 2019 onward or later) in order to provide a realistic statistical overview of the IoT landscape".

BEREC is responsible with the continuous development of the EU market for electronic communication networks and services, by ensuring the proper application of legislation at national and EU level, and improvements of the internal market. In fulfilling its responsibilities, BEREC works together with the European Commission and the national regulatory authorities (NRAs) providing advice and assisting them in the application of the sectorial regulatory framework. In its 2018-2020 Strategy *[BEREC, 2017]*, BEREC emphasizes the role of electronic communication on market development and innovation and, in its 3rd Strategic Priority - "Enabling 5G and promoting innovation in network technologies" clearly sees network technologies and developments as having "the potential to directly change the way services are used and delivered, such as IoT, NFV/SDN, as well as the technologies that may play a part in enabling such changes, e.g. small cell deployment ...". The 5 priorities identified by BEREC in its strategy, all of them related to market development and stimulation of innovation including smart technologies, are the following:

- Responding to connectivity challenges and to new conditions for access to high-capacity networks;
- Monitoring potential bottlenecks in the distribution of digital services;
- Enabling 5G and promoting innovation in network technologies;
- Fostering a consistent approach of the net neutrality principles;
- Exploring new ways to boost consumer empowerment.

In November 2019 BEREC ended 2 important public consultations, one on BEREC Work Programme 2020 and call for input to the BEREC Medium Term Strategy 2021-2023 (BEREC, 2019, Consultation on work programme 2020 and MTS), and the second on BEREC Guidelines on the Implementation of the Open Internet Regulation (BEREC 2019, Consultation on Open Internet) – the results are not published at writing time. Both of them are of great importance for the future of Internet, the development of electronic communication market and innovation in the European Union, with deep influence on the development of smart technologies as well.

It is also important to observe that the European Telecommunications Standards Institute (ETSI) issued, at the time of writing, less than 250 standards that are related to 2 of the most common smart technologies (more than 200 standards directed or related to Internet of Things, more than 30 standards to SCADA). ETSI is recognized as a European Standards Organization (ESO), is a non-profit organization established by the European Conference of Postal and Telecommunications Administrations (CEPT) in January 1988, and is officially recognized and partially funded by the European Commission and the European Free Trade Association (EFTA). ETSI has more than 850 member organizations from 65 countries. Romania is represented in ETSI by 4 organizations, all of them private companies in research, manufacturing and network provision areas. ETSI is responsible with the standardization in the ICT sector within the European Union and has 29 technical working Committees drafting and approving standards, performing consultations and updating them. Currently a lot of work is directed, or related to smart technologies, from electronic communication standards, to M2M languages, security, energy efficiency, EMC, interoperability, etc. With more than 20 thousands standards and recommendations issued every year, the number of standards related to smart technologies is still small, and more standardization need to be enforced, but considering the work in progress relevant results are expected in the following years.

It is important to mention the fact that all above represent a part of the actions undertook by the European Commission or other relevant communautaire bodies with regard to smart technologies. Also, part of the regulations issued during the 2000s were superseded by more recent regulations, as needed. As well, the aspects raised especially in ENISA reports, will be discussed in more detail furthermore.

Considering mature technologies such as SCADA, at national level ASRO (Romanian Association for Standardization) issued a limited number of standards, mainly related to measuring and control equipment for power grids, gas pipes, water distribution, generally large distribution networks for public utilities. We couldn't find any standard dedicated to IoT or IIoT approved at national level. Existing standards usually represent adoptions of ETSI standards and deals with safety and electromagnetic compatibility (e.g. SR EN 60255-22-1:2008, SR EN 60255-22-2:2008, SR EN 60255-22-3:2009, etc.), environment conditions (e.g. SR EN 60870-2-2, etc.) or data transmission (e.g. SR EN 60870-5-01:2004, SR EN 60870-5-04, SR EN 60870-5-101, SR EN 60870-5-103, SR EN 60870-5-104, SR CEI/TS 61850-2:2006, SR EN 62361-2:2014, etc). A technical specification regulating the design of informatics systems for the national power grid (PE 029/97) must also be mentioned. Similarly, there is no regulation issued at national level on smart technologies, being SCADA, or IoT, or others. The regulatory framework on safety of electric/electronic equipment, electromagnetic compatibility, data transmission, environment, and cyber security is, however, very elaborated and harmonized with the equivalent European regulatory framework.

CONCLUSIONS

Businesses used smart technologies for decades mostly in production environments and public utilities distribution. In the last decade public administrations intensely implemented smart systems in the benefit of the communities they serve. Directly or indirectly, smart technologies serve, nowadays, the life and activity of every citizen, member of a larger human community, even if we are not aware of this fact. The more we leave these technologies in our lives, the more we have to be aware of the aspects that, implicitly or not, they can bring into our physical lives. Among these aspects, from a business point of view the most important probably relate to increased productivity and abundance of all types of products on the market, as well as important cost reductions. From a citizen's point of view, improvements in living conditions and lifestyle are probably more relevant. Public safety, health, public infrastructures management, are other areas seeing significant improvements from the use of smart technologies. Still, intensive use of technology bring along types or risks unaccounted before, like privacy, cyber security, production processes alteration, loss of data, etc., risks that needed urgent response from governments. In the EU, as can also be seen above, ENISA is one of the most active actor, actively dealing with all aspects involving the protection of data and ICT infrastructures, in close collaboration with national responsible institutions. Despite all measures, governments, businesses and common people are permanently challenged, and the threat for cyber security incidents is constant. Protection of data and ICT infrastructures is one of the most innovative domain in our modern economy in both its aspects: incidents, and response to incidents. Therefore, we consider necessary to strictly regulate some of the aspects related to smart technologies (such as safety, physical and virtual security, privacy, personal data usage etc.), while others may remain loosely regulated (e.g. data exchange, interoperability, energy consumption etc.) or even unregulated (e.g. design, accessibility, usability etc.). While aspects like product design or usability are subject to personal tastes, others like safety, security or privacy needs to ensure an acceptable level of risk to all users of smart technologies, physical persons in their both, real and virtual life, as well as to businesses and public administrations in their activity.

Therefore, considering all above, we may conclude that smart systems are complex systems made of digital and analogue elements, and intended to monitor and control, to manage target environments and systems, usually functioning as open systems, responding to a demand in improved functionalities and to a demand in risk management.

As it may easily be seen, smart systems have an implicit modular structure at both, the physical (sensoring, hardware equipment, control and command elements etc.) and logical layers (software, procedures, methodologies etc.). Each module may function independent to the others, and each module may fulfill its purpose without depending on the others. As examples we may have the data collection module, the processing and reporting module, the storage and archiving module etc. – each of them may function independently, without correlations or dependencies. Still, the proper functioning of the integrated smart system depends upon both, the proper functioning of all modules, as well as their inter-dependent and correlated work together. The internal relationships ensures the fact that, considering the system's purpose, relevant results from the smart system are obtained from the inter-dependent work of its all components and the inter-dependent processing of data inside the components. Commonly, the output of a module becomes input for a different module, all repeated in infinite loops to fulfill the basic monitoring and controlling functionalities of the smart system. Similarly, each module, each component carry particular risks that cumulate with, sometime unpredictable consequences, at system level, and needs to be approached in equal measures on all layers.

As we already mentioned, from the functionalities' point of view we may consider the ensemble formed of the target environment or system, and the smart system, as an open, self-regulated system, where the smart (controlling) system plays in the self-regulating loop. Considering the type and functionalities of the smart system it may have, usually, a feedback loop role or, in particular situations, feed-forward loop. While in a feedback loop the system analyses the effect control commands have on the target environment or system, in a feed-forward loop commands are applied in a more automated manner estimating the effect commands will have on the target based on previous knowledge on the latter. As Karl Johan Åström, Richard M. Murray explain *[Åström and all, 2008]*, "Feedback is reactive: there must be an error before corrective actions are taken. However, in some circumstances, it is possible to measure a disturbance before the disturbance has influenced the system. The effect of the disturbance is thus reduced by measuring it and generating a control signal that counteracts it. This way of controlling a system is called feed-forward." While in feedback loops measured parameters' values are used to determine the type and amplitude of control elements' adjustments to bring the system within the accepted limits, feed-forward loops are characterized by following known patterns and changing parameters estimating the impact beforehand, not necessarily measuring it afterwards. Both approaches may be applied to smart systems, being only a matter of implementation considering the needed control of the target system or environment. Regarding these aspects, is obvious that common rules, data exchange and electronic interoperability are similarly important to all other functional or security aspects, and common rules and standards need to be followed by equipment producers at global scale.

Considering all above, becomes increasingly clear that integrated smart systems are complex system that must be considered in a multi-disciplinary approach both in terms of implementations (e.g. domestic, commercial, or public administration levels), and management, and the risks they bring upon target environments or systems, as well as people using them. It does not provide sufficient cover to let the market entirely decide what steps should be taken considering the balance between functionality and risk (i.e. equipment usage vs privacy concerns), policies and regulations must be enforced in securing people and businesses' data, and the objectives to protect them should be pursued by all significant actors, respectively governments, private companies and the civil society.

REFERENCE LIST

Alliance for Internet of Things Innovation (AIOTI), https://www.aioti.eu

Alliance for Internet of Things Innovation (AIOTI), Report on workshop on security and privacy in IoT, January 2017

Body of European Regulators for Electronic Communications (BEREC), BEREC Strategy 2018-2020, BoR (17) 175, October 2017

Body of European Regulators for Electronic Communications (BEREC), Internet of Things indicators, BoR (19) 25, March 2019

Body of European Regulators for Electronic Communications (BEREC), BEREC public consultation on its Work Programme 2020 and call for inputs to MTS

Body of European Regulators for Electronic Communications (BEREC), Public consultation on the document on BEREC Guidelines on the Implementation of the Open Internet Regulation

Body of European Regulators for Electronic Communications (BEREC), Report "Enabling the Internet of Things", BoR (16) 39, February 2016

European Network and Information Security Agency (ENISA), https://www.enisa.europa.eu

European Network and Information Security Agency (ENISA), Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017

European Network and Information Security Agency (ENISA), Good Practices for an EU ICS Testing Coordination Capability Report, December 2013

European Network and Information Security Agency (ENISA), Good practices for Security of Internet of Things in the context of Smart Manufacturing, November 2018

European Network and Information Security Agency (ENISA), Industry 4.0 Cybersecurity: Challenges & Recommendations, May 2019

European Network and Information Security Agency (ENISA), IoT Security Standards Gap Analysis v1.0, December 2018

European Network and Information Security Agency (ENISA), IoT Security Team, Introduction to IoT security – Forth NIS Summer School 2018

European Network and Information Security Agency (ENISA), Protecting Industrial Control Systems, Recommendations for Europe and Member States, 2011

European Network and Information Security Agency (ENISA), Towards secure convergence of Cloud and IoT, September 2018

European Commission portal, COM(2009) 149 final; Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", 2009, European Commission

European Commission portal, COM(2010)245 final; Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions "A Digital Agenda for Europe", 2010, European Commission

European Commission portal, COM(2015) 192 final; Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, "A Digital Single Market Strategy for Europe" 2015, European Commission

European Commission portal, COM(2016) 176 final; Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions "ICT Standardisation Priorities for the Digital Single Market", 2016, European Commission

European Commission portal, Commission implementing Decision (EU) 2018/637 of 20 April 2018 amending Decision 2009/766/EC on the harmonisation of the 900 MHz and 1 800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community as regards relevant technical conditions for the Internet of Things, 2018, European Commission

European Commission portal, Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation, 2017, European Commission

European Commission portal, Shaping Europe's digital future, A European Strategy for Data; https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

European Commission portal, Shaping Europe's digital future, Digitising European Industry; https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry

European Commission portal, Shaping Europe's digital future, Internet of Things (Unit E.4); https://ec.europa.eu/digital-single-market/en/content/internet-things-unit-e4

European Commission portal, Shaping Europe's digital future, The Internet of Things; https://ec.europa.eu/digital-single-market/en/internet-of-things

European Commission portal, Study on mapping Internet of Things innovation clusters in Europe, Final Study Report, 2019; A study prepared for the European Commission DG Communications Networks, Content & Technology by The Joint Institute for Innovation Policy (JIIP), Joanneum Research Forschungsgesellschaft mbH, Fundación TECNALIA RESEARCH & INNOVATION, VTT Technical Research Centre of Finland and KPMG AG

European Commission portal, SWD(2016) 110 final; Commission Staff Working Document "Advancing the Internet of Things in Europe" accompanying the document Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions "Digitising European Industry, Reaping the full benefits of a Digital Single Market", 2016, European Commission

European Commission portal, SWD(2017) 500 final; Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 2017, European Commission

European Commission portal, SWD(2018) 137 final; Commission Staff Working Document "Liability for emerging digital technologies" accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions "Artificial intelligence for Europe", 2018, European Commission

European Union legislation portal, https://eur-lex.europa.eu

European Union legislation portal, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

European Union legislation portal, Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office

European Union legislation portal, Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010

European Union legislation portal, Regulation (EU) 2018/1971 of the European Parliament and of the Council of 11 December 2018 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Agency for Support for BEREC (BEREC Office), amending Regulation (EU) 2015/2120 and repealing Regulation (EC) No 1211/2009

European Union legislation portal, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act); Feedback Systems: An introduction for scientists and engineers, Karl Johan Åström, Richard M. Murray, Copyright © 2008 by Princeton University Press

Institute of Electrical and Electronics Engineers (IEEE), Three-layer PLC/SCADA system Architecture in process automation and data monitoring, The 2nd International Conference on Computer and Automation Engineering (ICCAE), 2010

International Society of Automation (ISA), 2005, “Integrator’s Corner: Automating with .NET and SCADA”

International Telecommunication Union (ITU), ITU-T Y.2060; Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks; Next Generation Networks – Frameworks and functional architecture models; Overview of the Internet of things, 06/2012, International Telecommunication Union

The European Telecommunications Standards Institute (ETSI), https://www.etsi.org