CPS/IoT Ecosystem: A platform for research and education

Haris Isakovic[1], Denise Ratasich[1], Christian Hirsch[1], Michael Platzer[1], Bernhard Wally[1], Thomas Rausch[1], Dejan Nickovic[2], Willibald Krenn[2], Gerti Kappel[1], Schahram Dustdar[1], and Radu Grosu[1]

[1] Technische Universität Wien, Austria
[2] Austrian Institute of Technology, Austria
{name.surname}@tuwien.ac.at {name.surname}@ait.ac.at

Abstract. The CPS/IoT Ecosystem project aims to build an IoT infrastructure that will be used as a platform for research and education in multiple disciplines related to CPS and IoT. The main objective is to provide a real-world infrastructure, and allow students and researchers explore its capabilities on actual use cases.

Keywords: Internet-of-Things · Infrastructure · Cyber-Physical System

1 Introduction

We are experiencing a major paradigm shift in terms of computing systems. The ability to collect big data, use it to model physical environments with astonishing precision and use it to improve existing systems is a principal factor behind the upcoming revolution.We are using Cyber-Physical Systems(CPS) to observe and manipulate our physical environment,and the Internet-of-Things (IoT) to transfer and transform this raw data into profitable information.CPS/IoT Ecosystem is a project that materializes this idea. It embodies an infrastructure for IoT integrated together with a set of use cases that represent CPS. It is a joint project of three research institutions Technische Universitẗ Wien (TU Wien), Austrian Institute of Technology (AIT), and Institute for Science and Technology (IST). It serves as a research platform for a variety of related disciplines and as an educational tool for bringing concepts of IoT and CPS closer to the students in a "hands-on" type of an approach.

The preliminary forecasts state that IoT it will continue to grow rapidly in the next ten years. Multiple studies predict a number of new IoT devices to reach 75-100 billion until 2025 [20]. The global network of IoT devices will include both public and private IoT domains, with the ability to share and monetize not only results but also the usage of the infrastructure itself [8] [15]. We will highlight just few important challenges:

Development. Each scope of operation ion CPS and IoT (e.g., cloud, fog/edge, sensor, network) is traditionally observed as a separate discipline.The development methods and tools for each scope have been created accordingly

and they are not necessarily mutually compatible. To build an IoT application the tools for development, testing, and deployment need to be fully inter-operable.

Management. The holistic idea of IoT is to have billions of heterogeneous devices serving millions of different applications connected to Internet. Running these systems requires configuration, deployment, software updates and maintenance etc. Managing these tasks on a system this magnitude is a major challenge and requires enormous amount of effort.

Security. In the world where "every single thing" is connected to the Internet, security represents crucial requirement. Standardized approach to security and related topics, i.e., privacy and trust must be is a major challenge in IoT. Example from data breaches and recent changes in EU regulation regarding handling private data [26] highlights just how important is security in IoT. In the future data will influence policies and indirectly lives of people. Making sure that the data is valid and secure is extremely important.

Power Consumption. Over 75 billion new devices in just under ten years will create a massive overhead on the existing power infrastructure. The current production of electrical energy in the European Union on a yearly basis is around 3000 TWh [6].An average IoT device like the Raspberry Pi 3 consumes up to 5 Wh of electrical energy.If we pessimistically project it onto new IoT devices we get 3240 TWh on a yearly basis just for these devices.

The project will focus on implementing hardware structure of devices with custom build cloud system, fog/edge nodes, and COTS and custom built sensor and actuator devices that will form an infrastructure. It explores development frameworks, tools and mechanisms that will ensure standardized design and help establish functional system between hardware, software, and applications. A major aspect of the project is its educational value in terms of bringing state-of-the-art technology directly into curriculum. A new IoT infrastructure providing means for realistic implementations and applications, it enables students to experience complexity, real-time, security and dependability issues on real-world examples. Beside using the infrastructure in courses, the infrastructure will become central topic for numerous bachelor and master theses.

In this chapter we introduced the motivation behind the project and its core concepts. In Chapter 2 we provide short overview of the related projects. Chapter 3 describes methodology for the project execution and its most essential components. Two use cases implemented in the project are described in Chapter 4. The final chapter concludes the paper and provides future directions for the project.

2 Related Work

IoT represents a super set of multiple disciplines i.e., machine learning, artificial intelligence, real-time systems, embedded systems, high performance computing, web and mobile technologies, networking , enterprise organization, civil engineering and a number of others. Vermessan et. al. define IoT as *"a concept*

and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals" [28]. In this section we will give a short overview of the relevant research topics with respect to the CPS/IoT Ecosystem project and related research projects within the scope of EU research community.

The heterogeneity of IoT is one of its most prominent features however on the development and run-time level it is often primary source of **interoperability** issues. This is why the interoperability is one of the most researched topics in IoT. A significant number of projects in are working to enable or increase interoperability between existing and new IoT platforms and devices [5, 14, 18].

Second major topic in the scope of IoT research and development is **security**. It is arguably the most difficult challenge in IoT. It is a rather complex topic, as it branches in a numerous subtopics, each pf which is highly complex and demanding on its own. Thus a large variety of projects and research initiatives on the variations of security and security related topics (e.g., encryption, trust, privacy, block chain, user, data and ip protection) [4, 19, 13, 23].

The IoT represents a large heterogeneous system with a enormous variety of applications. Providing generic rules and guidelines allows us to create systems with standardized system properties. However, systems also need to be tailored to each individual application and its requirements. According to Gabriel in [12] *"a system that can be customized, specialized, or extended to provide more specific, more appropriate, or slightly different capabilities"* is called **framework**. A framework allows us to use it for different purposes without having a need to write the code each time from the beginning. Multiple research initiatives are exploring different frameworks for IoT, with different specialization abilities (e.g., security, safety, service-oriented design, social aspect, education and others)[10, 19, 7, 23, 22, 25].

Providing generic rules and guidelines allows us to create systems with standardized system properties. However, systems need to be tailored to specific application requirements. According to Gabriel in [12] *"a system that can be customized, specialized, or extended to provide more specific, more appropriate, or slightly different capabilities"* is called **framework**. It allows us to use it for different purposes without having a need to write the code each time from the beginning. Building such systems is one of the most explored questions in IoT. Multiple research initiatives are exploring different IoT frameworks with different specialization abilities (e.g., security, safety, service-oriented design, social aspect, education and others)[10, 19, 7, 23, 22, 25].

The applications are strongest driver behind IoT revolution. IoT applications are normally spearheaded by commercial subjects and the number of different ways IoT is improving existing systems changes every day. The research aspects with respect to IoT applications focuses on model and framework design, big data, social and economical implications, security and privacy issues, and

cooperation with other fields of science (e.g., biology, medicine, mechanical engineering, geo-engineering, etc.) [2, 9, 18, 1].

3 CPS/IoT Ecosystem Methodology

CPS/IoT Ecosystem is conceived as a heterogeneous structure of hardware devices, and corresponding software components distributed over tree intertwined scopes of operation: cloud, fog/edge, and sensor/actuator nodes. The cloud provides high performance computation and large capacity storage. The fog, also referred as edge, level indicates a network of devices with real-time communication capabilities, and mid-range computational and storage capabilities. The sensor/actuator level serves as a direct interface with physical environment. They posses capabilities of collecting and transforming physical signals using sensors and manipulating the environment via diverse actuators. The CPS/IoT Ecosystem infrastructure is a geographically distributed system. Parts of the infrastructure will be located on multiple sites on a wider area of Vienna,Austria.

CPS/IoT Ecosystem Cloud The cloud system is a general purpose high-performance computing platform located at a server center of TU Wien. It provides services that facilitate handling of big data (e.g., storage, analysis, aggregation). It is an essential part of the infrastructure. In CPS/IoT Ecosystem we are implementing a custom built cloud server. Its purpose is to serve the applications, but also to be used as a research subject. It will be deployed in two parts: a) a general purpose computing platform, and b) specialized computing platform for calculation intensive tasks.

CPS/IoT Ecosystem Fog/Edge Ability to react fast and ensure quality of service (QoS) on a factory floor level or similar plane of execution is implemented in the fog/edge level. It represents a network of computing nodes which are both capable of handling certain significant of data and still ensure service dependability. The fog/edge devices can be in direct connection to the sensor/actuator nodes or as an intermediate gateways for the ultra low energy/performance devices.

CPS/IoT Ecosystem Sensor Device The sensor/actuator nodes are direct interfaces with a physical environment. These devices are limited in computational performance, size and power consumption. They can be deployed individually or in swarms as explained in Section 4.

CPS/IoT Ecosystem Information Model As mentioned above management, development, and security are three major challenges in IoT. Part of the solution for these challenges is a functional IoT information model for the CPS/IoT infrastructure. It will allows us to describe the system from multiple perspectives: hardware platform, services, application, management and communication. The acquired models can be used as templates for application design, code generation, development and operations (DevOps), testing and validation.

COTS vs. Custom Built Hardware CPS/IoT Ecosystems generally comprises a substantial amount of sensor nodes.Buying a lot of sensor hardware can quickly consume an important amount of a project's budget, since commercially available ready to use hardware is usually expensive. Therefore designing and building custom hardware can be an attractive alternative. Designing custom hardware also has the advantage of increased flexibility, since one is not limited by the choice of existing components. The hardware design can be tailored to specific requirements as described in 4.

Technology in CPS/IoT Ecosystem The objective of the CPS/IoT Ecosystem project is to build a technology agnostic IoT infrastructure. Often the IoT is connected to a single framework, communication protocol or cloud environment. This project will provide general purpose cloud environment based on OpenStack[24]. It uses variety of open source and research community frameworks to build middle-ware and application software [17, 10, 27, 11]. In CPS/IoT Ecosystem we are not limited to a single communication protocol, typical IoT communication standards described in [3, 16, 21] will provide a basis for networking and communication standards.

4 Use Cases

4.1 Smart Parking

Smart Parking application provides status information of public or private parking places in a city or garage. Each parking spot is equipped with a sensor or group of sensors capable of detecting objects (cars or similar) on a surface of the parking spot. Data of each sensor is then transmitted to a central application software located on a remote server via Internet connection. The information is further delivered to end user over Web or mobile application. The Smart Parking application is build on the principle of CPS/IoT Ecosystem. The cloud environment serves as mass storage device and a service provider to external users. It collects all parking information from the fog all fog nodes and provides them to external applications (e.g., web site). The edge/fog nodes serve as sensor data aggregation and filtering nodes. The data collected from the sensors is transformed in the application useful information. The parking spot is a virtual concept and can be formed on arbitrary surface with a single or multiple heterogeneous sensors. Figure 1 provides an architectural overview of the Smart Parking application. The middleware backbone of the Smart Parking application is a service-oriented Arrowhead IoT Framework[10]. The Smart Parking application services are distributed over local clouds both on cloud and edge/fog level of operation. Senor nodes are connected via Bluetooth Low Energy (BLE) protocol. Future work on this use case considers adding multiple additional services (e.g., payment, allocation and reservation of spaces), also adding support for multiple sensor types and building vehicle-2-infrastructure interface for autonomous parking. Another feature is the implementation of sensor node simulator which is able to project sensors on the scale of the city and provide simulated data to the

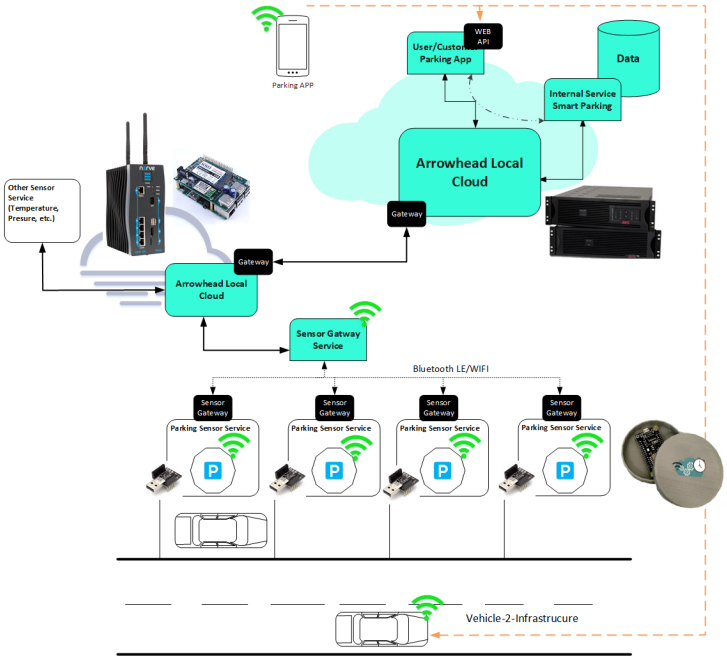

Fig. 1. Smart Parking Architecture Overview

rest of the infrastructure. This allows us to test scaleability and manageability of the application without deploying hardware devices.

4.2 Smart Vineyards

IoT can help to overcome arising problems in the agricultural sector. For example, the increasing labor shortage do to the depopulation of rural areas. This is possible because such infrastructures help farmers to work more efficiently. Examples are disease prediction systems, that warm farmers of arising diseases in certain areas. Farmers can use this information to bring out pesticides only when it is necessary and also only where it is necessary. This reduces the workload of farmers, the costs for pesticides and the negative impact on the environment.

We are building such an infrastructure for vineyards in cooperation with the Vienna University of Natural Resources and Life Sciences (BOKU Wien) as part of the CPS/IoT Ecosystem project. The aim is to bring out several hundreds of swarm nodes that measure the environment. This information is transmitted to the cloud via fog nodes. Later, the information is processed by means of big-data analysis and machine-learning algorithms to learn correlations between diseases and environmental influences to create new and improve existing diseases prediction models.

5 Conclusion

The paper provides a short overview of the CPS/IoT Ecosystem project and its main objectives. IoT has a complex and broad spectrum of topics and CPS/IoT Ecosystem is providing a platform where these topics can be explored and also bring closer to the students. Our goals are to build a physical infrastructure, to ensure data flow and application integration, demonstrate multiple use cases, and open it to other research initiatives for collaboration. The project is in its first stage and will continue to develop, thus our focus in the future will change on research of methods how to improve management, development, security and other properties.

6 Acknowledgment

This work has been conducted within a project that has received funding from the Austrian Government through the Federal Ministry Of Education, Science And Research(BMWFW) in the funding program Hochschulraum-Strukturmittel 2016 (HRSM).

References

1. AfarCloud: Aggregate Farming in the Cloud, `https://www.ecsel.eu/projects/afarcloud`
2. AGILE: Aircraft 3rd generation MDO for innovative collaboration of hetergeneous teams of experts, `https://www.agile-project.eu`
3. Al-Sarawi, S., Anbar, M., Alieyan, K., Alzubaidi, M.: Internet of things (iot) communication protocols: Review. In: 2017 8th International Conference on Information Technology (ICIT). pp. 685–690 (May 2017). https://doi.org/10.1109/ICITECH.2017.8079928
4. ARMOUR: Large scale experiment of IoT security and trust, `https://www.armour-project.eu/`
5. BIGIoT: Bridging the Interoperability Gap of the Internet of Things, `http://big-iot.eu`
6. BP: Bp statistical review of world energy. bp-statistical-review-of-world-energy-2017-full-report.pdf (June 2017), `https://www.bp.com/content/dam/bp/en/corporate/pdf/energy-economics/statistical-review-2017/bp-statistical-review-of-world-energy-2017-full-report.pdf`
7. Brain-IoT: A model-Based Framework for dependable sensing and Actuation in Intelligent decentralized IoT systems, `http://www.brain-iot.eu`
8. Chen, S., Xu, H., Liu, D., Hu, B., Wang, H.: A vision of iot: Applications, challenges, and opportunities with china perspective. IEEE Internet of Things Journal **1**(4), 349–359 (Aug 2014). https://doi.org/10.1109/JIOT.2014.2337336
9. CLOUT: Cloud of Things for empowering the citizen clout in smart cities, `http://clout-project.eu/`
10. Delsing, J.: IoT Automation: Arrowhead Framework. CRC Press (2017), `https://books.google.at/books?id=6mMlDgAAQBAJ`

11. FU Berlin: RIOT - The friendly Operating System for the Internet of Things. available at http://riot-os.org, accessed 2018-07-18
12. Gabriel, R.P.: Patterns of Software: Tales from the Software Community. Oxford University Press, Inc., New York, NY, USA (1996)
13. GhostIoT: Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control, https://www.ghost-iot.eu
14. InterIoT: Interoperability of heterogeneus IoT platforms, https://vicinity2020.eu
15. Kyriazis, D., Varvarigou, T., White, D., Rossi, A., Cooper, J.: Sustainable smart city iot applications: Heat and electricity management amp; eco-conscious cruise control for public transportation. In: 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). pp. 1–5 (June 2013). https://doi.org/10.1109/WoWMoM.2013.6583500
16. Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S., Sheng, Q.Z.: Iot middleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal **4**(1), 1–20 (Feb 2017). https://doi.org/10.1109/JIOT.2016.2615180
17. Open Source Robotic Foundation, Inc.: Robot Operating System (ROS). available at http://www.ros.org/, accessed 2018-07-06
18. Productive4.0: Electronics and ICT as enabler for digital industry1 and optimized supply chain management covering the entire product lifecycle, https://productive40.eu
19. RERUM: REliable, Resilient and secUre IoT for sMart city applications, https://ict-rerum.eu/
20. Rose, K., Eldridge, S., Chapin, L.: The internet of things: An overview. ISOC-IoT-Overview-20151221-en.pdf (Feb 2015), https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf
21. Schachinger, D., Kastner, W.: Semantic interface for machine-to-machine communication in building automation. In: 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). pp. 1–9 (May 2017). https://doi.org/10.1109/WFCS.2017.7991956
22. Semiotics: Secure Multi-protocol Integration Bridge for the IoT, https://www.semiotics-project.eu
23. SerIoT: Secure and Safe Internet of Thing, https://seriot-project.eu/
24. Shrivastwa, A., Sarat, S., Jackson, K., Bunch, C., Sigler, E., Campbell, T.: OpenStack: Building a Cloud Environment. Packt Publishing (2016)
25. SOCIOTAL: Creating a socially aware citizen-centric Internet of Things, http://sociotal.eu/
26. THE EUROPEAN PARLIAMENT: Regulation (eu) 2016/679 of the european parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679\&from=DE
27. Thingsboard: Thinsboard IoT Platform, https://thingsboard.io/
28. Vermesan, O.: Internet of things : converging technologies for smart environments and integrated ecosystems. River Publishers, Aalborg, Denmark (2013)