DOI: 10.1561/9781680838251.ch1

Chapter 1

Introduction

By Erkuden Rios, Nicolas Ferry, Hui Song and Andreas Metzger

Internet of Things (IoT) systems are evolving towards what we denote as Smart IoT Systems (SIS) – *i.e.*, systems involving not only sensors but also actuators with control loops distributed all across the IoT, Edge and Cloud infrastructure.

However, the capacity in building novel and innovative SIS faces specific challenges, that entail (i) how to efficiently build and operate new value-added software across IoT, edge and cloud infrastructures, (ii) how to close the loop of sensing and actuation, and (iii) how to establish trustworthiness in these systems. Whilst point (iv) is already critical in classical IoT systems: according to the IEC report on smart and secure IoT platforms [5], security, trust, privacy and identity management are major challenges in today's IoT systems, this is all the more exacerbated when actuators are involved.

One of the fundamental research questions concerning these issues is: "how can we tame the complexity of developing and operating smart IoT systems, which

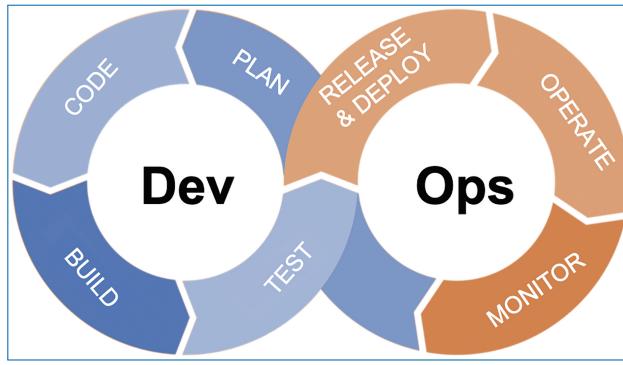

Figure 1.1. The generic DevOps life-cycle model.

(i) consist of software running on all types of resources along the IoT-edge-cloud continuum, (ii) involve sensors and actuators and (iii) need to be trustworthy?". The answer to these questions has formed the core of the Horizon 2020 project ENACT [1, 3]. The overall ambition of ENACT was to expand current DevOps methods and solutions to support the development and operation of trustworthy Smart IoT Systems.

DevOps has established itself as a software development life-cycle model that encourages developers to continuously patch, update, or bring new features to the system under operation without sacrificing quality [8]. By enabling DevOps in the realm of SIS, ENACT not only facilitates the development and operation of SIS but also enables the continuous and agile evolution of SIS, which is necessary to adapt the system to changes in its environment, including such as newly appearing trustworthiness threats. ENACT supports DevOps practices during the development and operation of trustworthy smart IoT systems by offering software tools, called "enablers", for each of the seven stages of the DevOps life-cycle model as depicted in Figure 1.1.

- **Plan:** ENACT supports privacy and security risk assessment enabling the risk-driven planning of IoT systems development cycles as well as the smooth transition towards the code stage.
- **Code:** First, ENACT evolves recent advances of the ThingML language and generators to support modelling of system behaviours and generation of code executable across the whole IoT, edge and cloud continuum. Second, ENACT provides a model-based solution to automatically identify and solve conflicts when multiple applications manage actuators.
- **Test:** Targeting the constraints related to the distribution and infrastructure of IoT systems, ENACT enables continuous testing of SIS in an environment by emulating and simulating IoT and Edge infrastructures.

- **Release and Deploy:** ENACT provides novel deployment modelling languages and the corresponding execution engines to support the continuous and automatic fleet deployment, by assigning multiple deployments to many devices in the fleet, without human interaction. It enables deployment from the IoT to the cloud ends with security as a first-class concern.
- **Operate:** ENACT provides enablers for the automatic adaptation of IoT systems based on their run-time context, including smart preventive security mechanisms such as access control. In addition, ENACT offers machine learning capabilities at runtime in order to deliver self-adaptive SIS. Such automatic self-adaptation addresses the issue that the management complexity of open-context IoT systems exceeds the capacity of human operation teams, and by this, improve the trustworthiness of the smart IoT system execution.
- **Monitor:** ENACT has delivered innovative mechanisms to observe and analysis (i) the status of a SIS including security and privacy aspects at all the network, system, and application levels, (ii) failures, (iii) the overall effectiveness of the SIS in reaching its goals.

ENACT was part of a cluster of related H2020 projects all contributing to IoT security [2]. Among the eight projects that formed the cluster, two are most notably related to ENACT and share common objectives. The Semiotics project[1] also considers SIS with a specific focus on the management of actuators. The project proposes a pattern-driven framework, built upon existing IoT platforms, to enable and guarantee secure and dependable actuation and semi-autonomic behaviour in IoT applications. While not specifically focusing on DevOps, one of the technical objectives of the Brain-IoT project[2] was to facilitate the rapid model-based development, integration, and deployment of interoperable IoT solutions that support smart cooperative behaviour involving actuation in IoT scenarios.

This book describes the ENACT project outcomes (cf. Figure 1.2) and how they solve major challenges in the DevOps of trustworthy SIS. The overall approach pursued in the ENACT project is introduced in Chapter 2, and the chapters following afterwards detail the outcomes of ENACT. In Chapter 3 the privacy and security risk assessment and management in SIS is discussed, and the ENACT enabler dealing with risks is presented. Chapter 4 is focused on deployment support offered by ENACT and the deployment and diversification methods and enablers are detailed therein. Chapter 5 deals with the issues of actuation conflict resolution in SIS that

1. https://www.semiotics-project.eu
2. http://www.brain-iot.eu

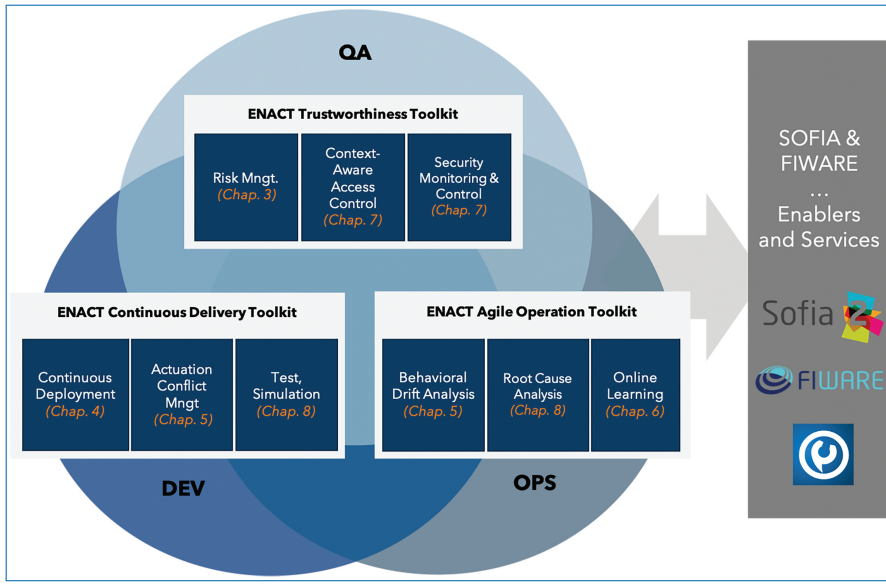

Figure 1.2. ENACT project results.

include actuators, and how to detect and analyse behaviour deviations at SIS operation from those designed when building the SIS. In Chapter 6 reinforcement learning techniques are studied as the ENACT approach for continuously ensuring and improving the quality of SIS during operations. Chapter 7 explains all the details of the ENACT support to security aspects of SIS, including context-aware access control enabler, security monitoring enabler, as well as security control through capabilities embedded in IoT platforms. Chapter 8 describes the ENACT enablers dedicated to the SIS verification and validation activities, including the support to testing, simulation and root cause analysis. Chapters 9, 10 and 11 explain the real IoT system use cases where the ENACT enablers were validated, dedicated to eHealth, Intelligent Transport Systems (ITS) and Smart Buildings domains, respectively. Chapter 12 concludes the book with an outlook on future research challenges and opportunities.

References

[1] ENACT Consortium. *ENACT: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems*, 2018. URL: https://cordis.europa.eu/project/id/780351.

[2] Enrico Ferrera *et al.* "IoT European security and privacy projects: Integration, architectures and interoperability. In: *Next Generation Internet of Things. Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation* (2018).

[3] Nicolas Ferry *et al.* "ENACT: Development, operation, and quality assurance of trustworthy Smart IoT Systems". In *International Workshop on Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment.* Springer. 2018, pp. 112–127.

[4] Jez Humble and David Farley. *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation*. Addison-Wesley Professional, 2010. ISBN: 860-1401501176.

[5] IEC. *IEC White Paper: IoT 2020: Smart and secure IoT platform*. IEC report, 2019. URL: https://basecamp.iec.ch/download/iec-white-paper-iot-2020-smart-and-secure-iot-platform/.