The overall research question behind the ENACT project is how to develop and operate software for the next generation IoT systems, which realize distributed and coordinated intelligence among large scale resources with closed-loop from sensing to actuation. The functioning and correctness of such
systems is critical, and aspects related to trustworthiness are of paramount importance. The vision of such trustworthy smart IoT systems (SIS) relies on advanced software services running across the IoT, Edge, and Cloud continuum, bringing the required intelligence to the devices and assuring the trustworthiness of the whole system. To enable the agile and continuous delivery of SIS is the key factor for the success of SIS application providers in order to keep competitive in the rapidly changing market. It is also fundamental to ensure the trustworthiness of SIS: In the world of IoT, new vulnerabilities keep emerging, and fast and continuous patching is a key approach to reducing the time that SIS are exposed to the risk of such vulnerabilities being exploited. Achieving trustworthy SIS is important not only to the IoT industry but also to society in general. By 2020, Gartner envisions that 21 billion IoT endpoints will be in use, representing great business opportunities for the entire ecosystem. In the meantime, IoT has infiltrated almost every aspect of modern living, significantly increasing the quality of our everyday lives, and any risk of trustworthiness in IoT systems may have a huge societal impact.

The overall goal of the ENACT project is to provide a novel way of developing and operating software for IoT, by enabling DevOps in the realm of trustworthy smart IoT systems. DevOps is a recent software development practice that encourages developers to frequently commit changes, and continuously place them in production. Despite its wide adoption in cloud computing, DevOps for IoT is still in its infancy. The state of the art on DevOps methods and tools relies heavily on the centralized, predictable and homogeneous resources to achieve fully automated deployment and operation, however, IoT breaks these assumptions.

ENACT investigated and experimented: (i) New practices: Three IoT solution providers transformed their daily development practice gradually into DevOps. In particular, the DevOps practice has supported the significant growth of one of the three use case providers, Tellu, in the eHealth domain. (ii) New techniques and tools: Researchers collaborated to attack the key challenges that hinder the implementation of this practice. This resulted in 10 software tools, the ENACT enablers, as the main exploitable outcome of the project. (iii) New usages: All partners together promote the acceptance of the new concept in the industry, and facilitate the adoption of the practices and tools by external IoT solution providers. Three companies from the project will provide commercial solutions based on the enablers, including a start-up company established during the ENACT period.

The results of the project demonstrate the feasibility and benefit of adopting the new DevOps practice in the domain of trustworthy smart IoT systems. It also demonstrates the importance of supporting such software engineering research in the domains that are traditionally considered as hardware-driven, such as IoT.

Work performed from the beginning of the project to the end of the period covered by the report and main results achieved so far

During the two periods, the ENACT consortium focused on (i) refining the challenges and requirements to achieve DevOps for trustworthy SIS based on three use cases, and then addressing them by the design and experiment of novel technologies; (ii) implementing these technologies into prototype or production tools and integrate the ENACT framework; (iii) evaluating the tools on the use
cases; and (iv) promoting the awareness and adoption of both the concept and the tools.

The project started with the definition of three use cases from the Intelligent Transportation, Smart Buildings and eHealth including their motivation as well as their business and technical requirements. Based on the use cases, the technical research and development activities of ENACT focused on addressing the key challenges that hinder the adoption of DevOps for trustworthy SIS: (i) the continuous delivery of trustworthy SIS, (ii) the agile operation of trustworthy SIS, (iii) and the trustworthiness mechanisms. The technical activities yield 10 ENACT enablers, or software tools:

- Continuous DevOps enabled Risk Management
- Automatic and Continuous, orchestration and deployment of Smart IoT Systems
- Actuation Conflict Management Tool in DevOps for trustworthy Smart IoT Systems
- An environment to simulate and test quality IoT systems
- Online Learning for Self-adaptive IoT Systems
- Behavioural Drift Analysis for trustworthy Smart IoT Systems
- Root cause analysis for security and performance issues
- Smart AI-Based IoT Security Monitoring and Control
- Context-aware Access Control tool for IoT
- Diversity-oriented fleet-level deployment and operation of IoT Systems

The ENACT consortium is active in disseminating the project and the latest results. The consortium follows the open source model. The tools are hosted in open source repositories, and SINTEF, on behalf of the consortium, is working together with OW2, an open source organization, to promote the external usage of the project results. The partners also follow up with their own exploitation plans to promote the results to the target users, i.e. the IoT application providers, along with the following three directions:

- Providing commercial products and services based on the open source tools
- Building communities for end-users to build their own DevOps environments
- Transferring knowledge and techniques to external partners.

Progress beyond the state of the art and expected potential impact (including the socio-economic impact and the wider societal implications of the project so far)

The ENACT concept and tools go beyond the state of the art. DevOps for trustworthy SIS is still a new concept and the adoption of the DevOps principles by IoT providers is still in its infancy. The ENACT use case providers are among the pioneers to actually transfer their daily development and operation practices according to the DevOps principles. ENACT provides a core reference DevOps toolchain to support the DevOps life-cycle for trustworthy SIS. The research behind these tools also advances the state of the art of their relevant domains, in different ways. In particular, for the continuous delivery of trustworthy SIS, we provide the first complete solution of automatic software deployment across Cloud, Edge and IoT devices, according to our systematic literature review; We introduce the continuous risk management into the DevOps loops of IoT systems, considering privacy and security issues. For the agile operation of trustworthy SIS, our initial experiment aims at raising the automation of IoT operation into the next level, by introducing online learning into the decision loop. For the
trustworthy mechanisms, we are a pioneer in supporting device-to-device authentication, with a context-aware control of the access rights.

The research has led to 40 scientific publications in the two periods, including 6 in good journals and 6 in A-level conferences. Two of the 6 A-level conference papers won the best paper awards. In addition, a book covering all the ENACT results will be published in July, 2021.