allocated on the FPGA fabric of modern cyber-physical system embedded processors.

The I3T architecture is associated with the network and end nodes of an IIoT infrastructure. We adopt industrial networks that use the TSCH operation of IEEE 802.15.4e and structure on top of it, a variation of the Zero-Touch Secure Join protocol [1] that enables the secure deployment of a new node in an IIoT network without user intervention. We further enhance this mechanism so that it can perform reconfiguration of the TSCH-6Top scheduling functions using secure CoAP messages. In parallel to that, we introduce a hardware/software co-design mechanism inside each IIoT end node SoC so that each device can support dynamic reconfiguration of its hardware resources. More specifically, the designer has available a series of hardware IP cores (with associated software drivers) that can be dynamically deployed after an application functionality analysis on the IIoT device. The analysis can highlight the computationally demanding operations that need to be accelerated by hardware in order to retain the IIoT real-time responsiveness and safety requirements. Target examples for hardware acceleration can be security/cryptographic primitive operations, and machine learning processing on fast and large time series data from the monitoring of electrical grid critical parameters or from machine and structural elements vibration sensors [3].

As an outcome of the above activities, we created an integrated, medium scale demonstrator for the smart energy and smart building environment, which includes widely used, wired and wireless, heterogeneous technologies of the relevant domains (e.g. BACNet, KNX, etc) which can also be attached to virtual environment simulators, in a hardware-in-the-loop fashion, capable of demonstrating the system operation at a larger scale. We have also designed and developed an IIoT node prototype that can support the I3T dynamic hardware accelerated reconfiguration and handle the TSCH software network stack (with all the proposed dynamic, zero touch secure I3T enhancements) [3].

Link:
[L1] https://i3t.isi.gr

References:
[1] M. Richardson: "6tisch Zero-Touch Secure Join protocol," Internet Engineering Task Force Draft
[2] C. Koulamas et al.: "IoT components for secure smart building environments", Springer, 2017
[3] A. Fournaris et al.: "Introducing Hardware-Based Intelligence and Reconfigurability on Industrial IoT Edge Nodes", IEEE Design & Test, 2019

Please contact:
Apostolos Fournaris
Industrial Systems Institute / R.C. "Athena", Greece
fournaris@isi.gr

Smart Municipality

by Jennifer Wolfgeher (FH Burgenland), Mario Zsilak (Forschung Burgenland) and Markus Tauber (FH Burgenland)

Digitalisation is already supporting individuals and smart cities in various ways. To increase automatization and digitisation, decisions must be based on trustworthy information. We are investigating the most common features of citizen participation and smart city platforms with the aim of determining the trustworthiness of the digital environment in this context.

Increased digitisation and automatization require applications that make it easy for citizens to report errors and be informed about possible incidents in their municipality. Such an incident management system can be citizen-based or automated via IoT (Internet of Things). An interaction between a citizen and the local authority may be to report an incident, e.g., an open manhole. An automated (IoT supported) version of this interaction would be the collection of relevant data from sensors. In any case, as actions are being triggered, both the citizen and the local authority needs information to be trustworthy.

Hence, on the municipality side, reliable and trustworthy data is essential, just as it is vital for citizens to know that they can rely on information they receive - such as disaster warnings. Trust is the most important requirement in emergency situations, in particular, but also in less extreme events like roadworks or construction areas. Existing smart city applications and citizen participation platforms provide features relevant for such scenarios.

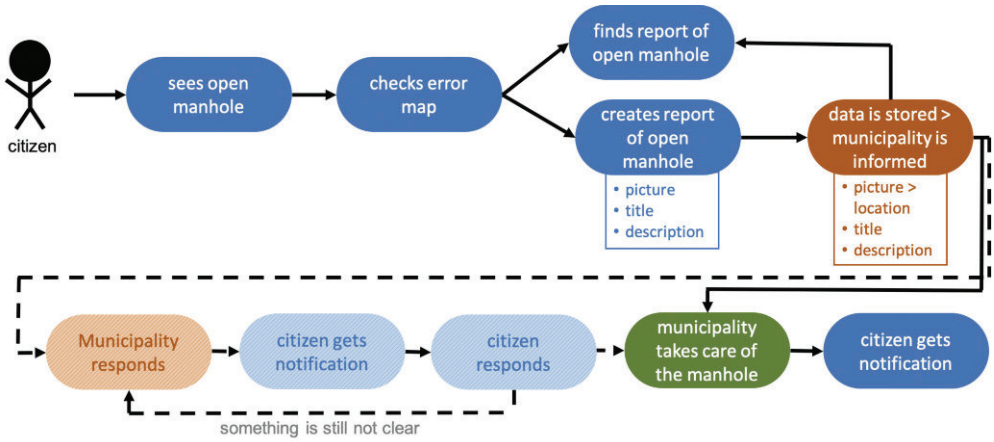
In the literature many platforms and applications have been investigated [1],[2] on the basis of their features and potential to enhance sustainability, but the need for security and trustworthiness is rarely addressed. This is reflected in real-life citizen participation and smart city platforms (e.g. platforms from Austria and Luxemburg, smart city projects from Stockholm and Singapore [L1-L4]). In these smart cities, the applications designed to increase citizen participation and make residents lives easier, rarely guarantee the reliability of exchanged information. Whilst including a number of useful features (like interactive maps, online participation in political discussions, waste service information and smart parking), no existing system provides incident management as an application in a trustworthy IoT environment. To enable reliable incident reports from citizens, information must be communicated to the municipality in a trustworthy manner, allowing the local authority to take action in dangerous situations (e.g. open manholes). On the citizen's side, only approved information about actual conditions from the municipality or sensors must be received, in order to ensure people's safety. Thus, a trustworthy framework to enable secure communication and to link individual services from existing heterogeneous platforms is required.

The Arrowhead framework [L5] is one example of a secure IoT framework that can integrate smartphones, sensors and external services in a smart city context. Sensors are already involved in the Arrowhead framework in different contexts, including industrial IoT (IIoT) and smart homes [L5]. This open-source framework provides many security functions by design, with the objective to facilitate security, reliability, real-time communication and safety in local cloud automation. With the chain of trust principle, it enables the usage of all services of the Arrowhead local cloud and the services of other clouds that are compliant with the Arrowhead framework, based on a secure on-boarding procedure.

In addition to the security advantages, Arrowhead supports a multi-cloud solution that would make it possible to stick together the "patchwork" of applications for smart city and citizen participation projects, e.g. the many applications of the smart nation of Singapore [L4] could be accessed via one service. The citizen could find the waste service as well as the parking service or tax service in one place. The applications could be in one cloud or distributed in separate, Arrowhead compliant, clouds, but the chain of trust would still be available from the citizen to each service.

The Arrowhead framework provides a chain of trust via various mechanisms, including certificates and secure on-boarding [3] to enable a trustworthy environment. Arrowhead is a fitting framework for the deployment of an incident report service in a trustworthy environment, capable of meeting the objectives of security, reliability, real-time communication and safety.

Figure 1: Use case - incident report.



Further research, in the EFRE project "civis 4.0 patria" (FE07) will include the actual deployment of an incident management feature considering frameworks like Arrowhead to support the development of smart municipalities.

Links:

[L1] https://www.buergermeldungen.com
[L2] https://kwz.me/hEN
[L3] https://kwz.me/hEe
[L4] https://www.smartnation.sg
[L5] https://www.arrowhead.eu/

References:

[1] O. Gil, M. E. Cortes-Cediel, I. Cantador: "Citizen participation and the rise of digital media platforms in smart governance and smart cities", Int. Journal of E-Planning Research (IJEPR), 8(1), 19–34, 2019.
[2] A. M. Pozdniakova, et al.: "Smart sustainable cities: The concept and approaches to measurement", Acta Innovations, (22), 5–19, 2017.
[3] A. Bicaku, et al.: "Interacting with the arrowhead local cloud: On-boarding procedure", in 2018 IEEE Industrial Cyber-Physical Systems (ICPS), pp. 743-748. IEEE, 2018.

Please contact:
Jennifer Wolfgeher
FH Burgenland, Austria
jennifer.wolfgeher@gmail.com

Teaching Sustainability and Energy Efficiency with the GAIA Project

by Georgios Mylonas (Computer Technology Institute & Press "Diophantus") and Ioannis Chatzigiannakis (Sapienza University of Rome)

Today's students are the citizens of tomorrow, and they should have the skills and tools to understand and respond to climate change. Green Awareness in Action (GAIA) has built an IoT infrastructure within 25 schools in Europe, in order to enable lectures that target sustainability and energy efficiency, based on data produced inside school buildings. The school community has reacted very positively to this approach and has reduced energy consumption as a consequence.

GAIA [L1], a Horizon2020 EC-funded project, has developed a large-scale IoT infrastructure in a number of school buildings in Europe. Its primary aim is to raise awareness about energy consumption and sustainability, based on real-world sensor data produced inside the school buildings where students and teachers live and work.

Overall, 25 educational building sites participated in GAIA, located in Sweden, Italy and Greece. The IoT infrastructure installed in these buildings monitors in real-time their power consumption, as well as several indoor and outdoor environmental parameters. However, this infrastructure would not be particularly useful without a set of tools to allow access to the data produced and provide functionality to sup-