# Interoperability for Disaster Relief Operations in Smart City Environments

Manas Pradhan

*Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE)*
Wachtberg, Germany
manas.pradhan@fkie.fraunhofer.de

***Abstract*—Internet-of-Things (IoT) technologies in the past decade have matured both in the hardware and software aspects for large-scale deployment. Alongst IoT, the Smart Cities Concept is also taking shape. Pilot projects and implementations in multiple cities are trying to find out the feasibility and applicability of Smart City Information and Communications Technology (ICT). IoT assets along with the legacy assets are essential for Smart City ICT implementations.**

**With the evolution of Smart Cities and concentration of people in the cities, it becomes necessary to be ready for future Humanitarian Assistance and Disaster Recovery (HADR) operations. But the huge void in heterogeneous IoT and legacy technologies create a big hurdle in establishing and handling the HADR operations. This aim of this PhD is to investigate the interoperability aspects amongst the various IoT technologies and Smart City concepts. The goal is to create a framework and an architecture for allowing the interoperable operation of ICT assets in a Smart City environment. This framework would enable rapid deployment of HADR relevant technology assets on the ground allowing multiple HADR agencies to seamlessly communicate while having shared Situational Awareness (SA) and complementing each others capabilities.**

***Index Terms*—IoT, Smart City, Interoperability, ICT, Civilian-Military Co-operation, Situational Awareness**

## I. Introduction

This PhD aims at investigating the technological heterogeneity in the domain of IoT with regards to Smart City and non-public ICT domains, and finding out interoperabilty aspects within and between these domains. The outcomes of the studies and investigation would provide the insight into reaching the goal of engineering an interoperable architecture and framework between the distinct ICT domains in a Smart City environment. The devised framework should enable multiple public (Smart City ICT) and non-public (Military, Police etc.) agencies to communicate and co-operate in HADR operations in a Smart City environment.

### *A. Background*

The world of Internet-of-Things (IoT) is the new revolution in the modern technology realm after the intrusion of Internet and mobile technologies. Gartner forecasts that there would be 20.4 billion IoT devices in use by 2020 and 125 billion by 2030 [1]. This surge in devices has led to the intrusion of IoT devices in everyday lives. Accordingly, technologies and applications to support these devices have also evolved immensely.

The IoT domain relies on the background concept of being connected to the internet or some kind of network to be able to perform actions on resource-constrained devices. These limitations on device size and capabilities have led to devising of network and communication protocols, data exchange mechanisms and Ontologies to be able to exploit the capabilities of these devices [2]–[4].

As the IoT domain has expanded, the concept of Smart Cities based on these newly available ICT standards, protocols and devices has also come into existence. These Smart Cities, by using these IoT technologies alongst the legacy devices, standards and protocols aim at making the lives of citizens in the cities better [5].

### *B. Problem Description*

Whilst the surge of IoT and Smart Cities has benefited the ICT development for the future generations, it has also led to the issue of interoperability between the existing (legacy) ICT systems and the systems based on IoT. The legacy assets can not be completely replaced with IoT systems [6], [7]. Thus the IoT assets need to co-exist with their associated legacy systems and exchange information with them.

The legacy systems use certain standards and protocols developed specifically for systems which are relatively much powerful (computationally) and have more or less reliable power supplies. On the other hand, IoT platform based systems, have different needs and capabilities and thus the supporting network and communication protocols, data exchange mechanisms and Ontologies are different [8].

This leads to the issue of the systems not being able to talk to each other. There is no standardized architecture or methodology which lets these systems co-exist or be easily interoperable either from the view point of [9]–[12]:

1) Network protocol usage for optimal operation of the hardware assets.
2) Data exchange mechanisms or standards, data models for defining optimal IoT assets utilization which are traditionally used for legacy assets.

This PhD study is supported by the German Ministry of Defence

978-1-5386-4980-0/19/$31.00 © 2019 IEEE

3) Service modelling based on Service Oriented Architecture (SOA) for the services to be running on the heterogeneous devices.
4) Ontologies that clearly define interactions between these heterogeneous devices in a Smart City environment.

Apart from the heterogeneity in the operation within the ICT systems, there lies a huge void in the way the public and non-public ICT domains work. Non-public ICT infrastructure assets belonging to governmental organizations like the police, fire services, military etc are engineered separately and also in most cases, ICT assets are kept separate from the public infrastructure used by the civilians [13], [14]. Traditionally, non-public ICT systems are not supposed or not designed to talk to commercial or public ICT systems [17], [18]. The information flow through these organizations is in most cases, sensitive and need to be kept isolated from the civilian domain due to security and confidentiality aspects. So, the communication networks, protocols, ontologies, data formats, physical assets (communication mediums, devices), syntax and semantics of information etc. in most cases is engineered differently as compared to the public ICT domains [16]. The information that needs to be made available to the public is filtered and examined before being allowed to be accessed by the public [15].

For a Humanitarian Assistance and Disaster Recovery (HADR) operation in a Smart City environment, the city's ICT deployment i.e. available devices and services can help the non-public organizations gain better SA [21]. So, in a Smart City scenario, non-public systems cannot talk i.e. be interoperable with the deployed Smart City assets. As Smart Cities have become the concentration point of human populations with their tangible and non-tangible assets, any incident, even on a small scale has large scale implications, both human-factor wise and economically [19]. Considering that disaster recovery operations need quick deployment of rescue assets and personnel, the non-interoperability of Smart City and non-public ICT systems will lead to non-assistance or reduced effectiveness of the rescue efforts and capabilities. And further on, delay in the HADR efforts will scale the magnitude of the disaster incrementally.

Based on [20], figure 1 shows the envisioned high level architecture for HADR Operations Interoperability in a Smart City Environment. The figure shows the ICT domains from HADR agencies and Smart City. These domains within themselves might employ IoT as well as legacy assets. Using a boundary gateway at the domain edges, they can inter-operate for a HADR operation for sharing information and assets to complement their capabilities.

Non-public organizations like the military have started looking into the idea of utilizing IoT for its operational requirements to either complement or replace the existing sensors, actuators, controllers, computers etc. Inclusion of the IoT devices means that the the non-public organizations need to extend the existing framework to adapt to the IoT-based network, data standards and protocols [22].

So, this creates two levels of problems:

1) How to make use of the recent IoT evolution to assist disaster recovery operations?
2) How to connect to the Smart City Domain in a disaster recovery scenario which contains legacy as well as IoT devices and technologies?

## II. Objectives and Entailed Scientific Work for PhD

The aim of the PhD is to device an architecture to enable data and semantic interoperability between the non-public ICT domain and, the IoT and Smart City domains. It aims towards making the involved heterogeneous components from the individual domains be ready to talk and deploy quickly in disaster recovery operations without extended discovery and configuration of the involved systems.

The following sub-sections describe the steps involved for the scientific work:

### A. Survey and Specification

In order to find out the existing technologies and its fallbacks, the Smart City ICT Infrastructures need to be analyzed in detail with regards to the available services, data, APIs and accessible devices across the European Union initiatives and other continents. This means that the systems and subsystems of smart city infrastructure needs to be identified including various processes and interactions between the components.

The current state and future directions of IoT domain, both public and non-public domains also needs to be analyzed to keep up-to date the IoT technologies w.r.t data exchange mechanisms, standards and protocols used, device maturity of the computers, controllers, actuators, sensors etc. In addition, the existing non-public ICT systems (ex. military C2 Systems), data exchange mechanisms, standards, protocols and the underlying architecture needs to be analyzed to be able to synthesize the existing non-public ICT capability and to extend the existing capabilities for interoperability. The result should be able to properly specify the factors that would drive the interoperability of the non-public systems with the IoT and Smart City domain.

### B. Case Studies, Implementation and Evaluation

*"The objective is to propose a unified, extendable and abstract framework for systems integration. This framework is to be deployed in actual proof-of-concepts and pilot deployments to ensure interoperability, which needs to be evaluated in the Smart City and IoT context"*. This means that the proposed methods and mechanisms will be applied against several components of Smart City and non-public (ex. military) ICT systems. Case studies would result in identifying challenges and parameters along with the validation of proposals. This would lead to identification of series of waypoints as the possible roadmap to go ahead to counter and overcome these challenges. The pilot implementations would provide the proof of the investigations, the approach used and the solutions being proposed to counter these challenges.

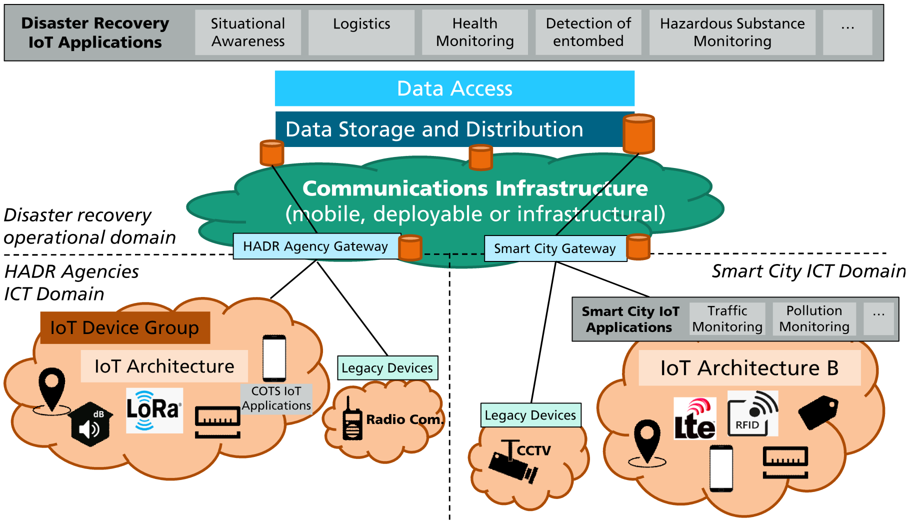

Fig. 1. High Level Architectural Overview for HADR Operations Interoperability [20]

### C. Analysis of Implementation

The framework developed will use real-time and latest verified and functioning Smart City and non-public ICT assets (APIs, services, devices) and the IoT components to visualize the functioning interoperability between the systems in the form of applications and services. The data visualization may be collected from the non-public C2 applications and services, IoT and/or Cloud services and end user applications.

## III. Scientific, Technological, and Social impact

The knowledge and impact that the PhD will gain and produce during the project can be summarized as:

1) Scientific Impact
   - Enabling interoperability between heterogeneous legacy and IoT-based ICT systems.
   - Generic Services engineering for disaster recovery operations which can be utilized by any rescue organization.
   - Understanding and bringing Smart City services from multiple countries and organizations under one umbrella for rapid deployment and utilization.
   - Bringing efficiency and optimize IoT-based protocols and technologies for future deployment in ICT systems.
   - Discover collaboration and opportunities for non-public systems to get involved with public systems.
   - Showcase proof and expansion of the realm of IoT device and technologies incorporation in non-public organizations operations.
   - Knowledge of Ontologies and, supporting Data Formats and Standards.
   - Knowledge of Data Exchange standards and protocols.
   - Knowledge of IoT in terms of specific protocols, standards services and devices.
   - Knowledge of distributed services: centralized cloud and Machine-to-Machine (M2M) infrastructures.
   - Knowledge of analyzing service requirements and Quality-of-Service (QoS).
2) Technological impact
   - Generic and common APIs for allowing public and non-public ICT systems to talk to each other.
   - Architecture for allowing multiple IoT protocols to talk to each other under the same platform.
   - Triggering use-case specific and on-demand services on edge devices to optimize and support disaster recovery operations.
   - Utilization of heterogeneous and multi-vendor sensors, actuators, controllers, C2 systems and edge systems to satisfy use-case specific operations.
   - Techniques for differentiating access using communication protocols for various service types.
3) Social Impact
   - Opening Smart City Services access for future disaster recovery operations and thus aid non-public organizations to save human and non-human resources in cities.
   - Showcase the benefits of IoT technologies for large-scale adoption within the public and non-public domains.
   - Allow the end-user humans to become a part of the Smart City operations and assist other HADR agencies in disaster recovery operations.
   - Faster and more precise disaster recovery operations supported by multi-tier organizations working in the same pretext.

## IV. PhD Study Milestones

The PhD would entail the following steps for achieving the envisioned aims and goals:

1) For architecture deliverable:

   - Study of the existing non-public (ex. military) data exchange techniques, standards and protocols.
   - Study of the existing public and non-public systems (Command and Control (C2), Edge systems etc.).
   - Study of the prevalent IoT devices and data exchange techniques (non-public and commercial).
   - Study of Smart City ICT approaches around Europe and other continents.
   - Study of IoT and Smart Devices (Smart Homes, Micro-controllers, Mobile Phone based applications etc.)
   - Study of Smart City APIs to discover and use the services offered by the Smart City.
   - Exploring concepts of crowd-sensing and crowd-sourcing, remote and mobile deployment of ICT services using edge computing etc.

2) For Integration Framework deliverable: Based on the studies for architecture deliverables, the following steps would commence:
   - Devising of an architecture to allow interoperability between military and non-military systems.
   - Devising an interoperable data model and ontology for public and non-public systems.
   - Development set of requirements for the integration framework.
   - Implementation of the framework for testing based on architecture devised.
   - Interoperability and usability tests of the implemented framework.
3) For Implementation System deliverable: The final stage of PhD would consist of the following steps based on the pilot implementation of the engineered interoperability framework:
   - Application of the developed pilot to an actual conglomerate of legacy and IoT systems in a Smart City environment as proof-of-concept.
   - Testing with the multiple agencies (public and non-public) and their systems involved to ensure that the proof-of-concept aligns to the engineered framework and the architecture goals.

   This would conclude and validate the PhD.

## References

[1] Gartner Says Smart Cities Will Use 1.6 Billion Connected Things in 2016. Gartner, Gartner Inc. , 7 Dec. 2015, www.gartner.com/newsroom/id/3175418.

[2] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

[3] Sheng, Zhengguo, et al. "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities." IEEE Wireless Communications 20.6 (2013): 91-98.

[4] Chandrasekaran, Balakrishnan, John R. Josephson, and V. Richard Benjamins. "What are ontologies, and why do we need them?." IEEE Intelligent Systems and their applications 14.1 (1999): 20-26

[5] Zanella, Andrea, et al. "Internet of things for smart cities." IEEE Internet of Things journal 1.1 (2014): 22-32.

[6] Bisbal, Jess, et al. "Legacy information systems: Issues and directions." IEEE software 16.5 (1999): 103-111.

[7] Park, Jinsoo, and Sudha Ram. "Information systems interoperability: What lies beneath?." ACM Transactions on Information Systems (TOIS) 22.4 (2004): 595-632.

[8] Da Xu, Li, Wu He, and Shancang Li. "Internet of things in industries: A survey." IEEE Transactions on industrial informatics 10.4 (2014): 2233-2243.

[9] Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010, December). Iot gateway: Bridgingwireless sensor networks into internet of things. In Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on (pp. 347-352). Ieee.

[10] Ahlgren, Bengt, Markus Hidell, and Edith C-H. Ngai. "Internet of things for smart cities: Interoperability and open data." IEEE Internet Computing 6 (2016): 52-56.

[11] Zhang, Y., Chen, J. L., & Cheng, B. (2017). Integrating Events into SOA for IoT Services. IEEE Communications Magazine, 55(9), 180-186.

[12] Hachem, Sara, Thiago Teixeira, and Valrie Issarny. "Ontologies for the internet of things." Proceedings of the 8th Middleware Doctoral Symposium. ACM, 2011.

[13] Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen national cyber security strategies." International Journal of Critical Infrastructures 6 9.1-2 (2013): 3-31.

[14] Waldrop, E. S. (2004). Integration of military and civilian space assets: legal and national security implications. AFL Rev., 55, 157.

[15] Ndou, Valentina. "EGovernment for developing countries: opportunities and challenges." The electronic journal of information systems in developing countries 18.1 (2004): 1-24.

[16] DeCleene, B., et al. "Secure group communications for wireless networks." Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE. Vol. 1. IEEE, 2001.

[17] Sigholm, Johan, and Dennis Andersson. "Privacy on the Battlefield?: Ethical Issues of Emerging Military ICTs." 9th International Conference of Computer Ethics: Philosophical Enquiry (17CEPE 2011), May 31st-June 3rd, 2011, Milwaukee, USA. INSEIT, 2011.

[18] Mjlnevik, Jon, and Urban Nuldn. "International military mobility and interoperability."

[19] Nam, Taewoo, and Theresa A. Pardo. "Conceptualizing smart city with dimensions of technology, people, and institutions." Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times. ACM, 2011.

[20] Johnsen, Frank T., et al. "Application of IoT in military operations in a smart city." 2018 International Conference on Military Communications and Information Systems (ICMCIS). IEEE, 2018.

[21] Hartama, D., et al. "Smart City: Utilization of IT resources to encounter natural disaster." Journal of Physics: Conference Series. Vol. 890. No. 1. IOP Publishing, 2017.

[22] Suri, Niranjan, et al. "Analyzing the applicability of internet of things to the battlefield environment." Military Communications and Information Systems (ICMCIS), 2016 International Conference on. IEEE, 2016.