भारतीय मानक
Indian Standard

IS 18000 : 2020

यूनिफाइड डिजिटल इन्फ्रास्ट्रक्चर — आईसीटी रेफेरेंस आर्किटेक्चर

Unified Digital Infrastructure — ICT Reference Architecture (UDI-ICTRA)

ICS 33.020, 35.020

© BIS 2020

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
MANAK BHAVAN, 9 BAHADUR SHAH ZAFAR MARG
NEW DELHI-110002
www.bis.gov.in www.standardsbis.in

December 2020 **Price Group 15**

For BIS use only, New Delhi:2021-01-08 16:08:56

Smart Infrastructure Sectional Committee, LITD 28

FOREWORD

This Indian Standard was adopted by Bureau of Indian Standards, after the draft finalized by the Smart Infrastructure Sectional Committee, had been approved by the Electronics and Information Technology Division Council.

The development of a series of standards for enabling a Unified Digital Infrastructure across the country was motivated by the Smart Cities initiative of the Government of India. A defining feature of Smart Cities is the ability of various components and systems to function efficiently in an integrated manner as well as independently. Unified, Smart, and ecure Digital Infrastructure will facilitate efficient integration of various Systems and Applications/Services across the city.

This standard provides a reference architecture and models for achieving such a unified digital infrastructure and can serve as a template for both the City Administrators, who are the consumers of such ICT based solutions, as well as the ICT Solution Providers who develop and deploy such solutions. The reference architecture described in this standard, while providing functional, technology, and information reference models, does not describe the implementation details.

The standard has been developed in collaboration with the Smart Cites Mission, Ministry of Housing and Urban Affairs (MoHUA), Government of India. During the preparation of this standard, several consultation meetings and discussions were held with a wide cross section of stakeholders. A few workshops were also organized for the Smart Cities with an objective to create awareness among the stakeholders, to discuss the technical details of the standard with them, and to get critical input from the representatives of several Smart City implementation entities. In addition, feedback was also sought from all the 100 Indian Smart City implementation entities at different stages of development of this standard.

All the diagrams, and key elements of the architecture are made/captured in Archimate 3.1, an enterprise architecture modelling language developed by "The Open Group", and the resulting files are available online in BIS Website and also in github and is a live representation of this architecture.

The standard was developed under the panel, LITD 28/P6 ICTRA that comprises experts from Academia, Industry, Government bodies etc. The composition of LITD 28/P6 and the committee LITD 28 responsible for the formulation of this standard is given at Annex E.

For BIS use only, New Delhi:2021-01-08 16:08:56

CONTENTS

For BIS use only, New Delhi:2021-01-08 16:08:56

Page No.

For BIS use only, New Delhi:2021-01-08 16:08:56

Page No.

FIGURES

For BIS use only, New Delhi:2021-01-08 16:08:56

Page No.

Tables

For BIS use only, New Delhi:2021-01-08 16:08:56

INTRODUCTION

A smart city is one that can effectively leverage technology, infrastructure, public policy, government and citizen engagement to create an urban environment that fosters economic growth and productivity, innovation, social mobility, inclusiveness, and sustainability.

Cities are complex entities having:

a) *Diverse Stakeholders*: Citizens, visitors, city administration, state government, central government, vendors, system integrators, business, academia, other organizations.

b) *Diverse Geographical Entities*: Parking lots, streets, buildings, electric stations, etc.

c) *Diverse Services and Business Processes*: With diverse functionality and consumers need to be developed.

d) *Diverse ICT Technologies*: Data systems, sensor technologies, software systems, networking systems etc.

While it is almost impossible to engineer a smart city from scratch, it will be possible to adopt the right architectural framework along with appropriate practices and policies to nudge the evolution towards smart cities.

The three key principles for facilitating such an emergence/evolution towards a smart city ecosystem are:

1) **Interoperability** — Refers to the ability of diverse systems and components to work together, even as parts from diverse set of suppliers are substituted and integrated;

2) **Composability** — Refers to the ability to combine discrete components into a complete system to achieve a set of goals and objectives; and

3) **Harmonization** — Refers to achieving compatibility between technologies and systems, even when they at first appear incompatible.

This standard provides a reference architecture for achieving such a unified digital infrastructure and can serve as a template for both the City Administrators, who are the consumers of such ICT based solutions, as well as the ICT solution providers who develop and deploy such solutions.

For BIS use only, New Delhi:2021-01-08 16:08:56

For BIS use only, New Delhi:2021-01-08 16:08:56

Indian Standard

UNIFIED DIGITAL INFRASTRUCTURE — ICT REFERENCE ARCHITECTURE (UDI-ICTRA)

1 SCOPE

1.1 This standard defines the reference architecture and models for information and communication technologies needed to realize a Unified Digital Infrastructure (UDI) in Smart Cities. The reference architecture includes functional reference models, technology reference models and information reference models. The standard offers a blueprint for realizing the unified digital infrastructure, but does not mandate any specific components. The reference architecture can be used to define various levels of architectural maturity, based on which components are included, from a basic level to an advanced level of the unified digital infrastructure. However, this categorization is not part of this standard.

1.2 The implementation details are also excluded from the scope of this standard.

2 REFERENCES

The standards given below contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of these standards:

Other Standards	*Title*
ISO/IEC/IEEE 4 : 2010	Systems and software engineering — Architecture description
ISO 8000 (Series)	Data Quality
ISO/IEC 20547 (Series)	Information technology — Big data reference architecture
ISO/IEC 11179	Information Technology — Metadata registries (MDR)
ISO 15000	Electronic Business Extensible Markup Language (ebXML)
ISO/IEC 20802 (Series)	Open Data Protocol (OData)
ISO/IEC 29161	Data structure — Unique identification for the Internet of Things
ISO/IEC 30182	Smart city concept model — Guidance for establishing a model for data interoperability
ISO/IEC 30182	Smart City Concept Model — Guidance for establishing a model for data interoperability
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27034-1 : 2011	Information technology — Security techniques — Application security — Part 1: Overview and concepts
ISO/IEC TR 24772 (Series)	Programming languages — Guidance to avoiding vulnerabilities in programming languages
NIST	Special Publication 800-53
PCI	Data Security Standard (PCI DSS)

3 TERMS AND DEFINITIONS

3.1 Terms and Definitions

For the purpose of this standard, the following definitions shall apply.

3.1.1 *Accessibility* — Extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of user needs, characteristics and capabilities to achieve identified goals in identified contexts of use.

NOTE — To entry: Context of use includes direct use or use supported by assistive technologies.

[SOURCE: ISO 9241-11:–, 3.1.14]

For BIS use only, New Delhi:2021-01-08 16:08:56

3.1.2 *Availability* — Property of being accessible and usable upon demand by an authorized entity. [SOURCE: ISO/IEC 27000 : 2016, 2.9]

3.1.3 Citizen — <of a city> person who lives and/or works, within a city.

3.1.4 *Composability* — The ability to combine discrete components into a complete system to achieve a set of goals and objectives. [Source: ISO/IEC 30141 : 2018, Modified]

3.1.5 *Confidential Computing* — The protection of data-in-use through isolating computations to a hardware-based trusted execution environment (TEE). While data is traditionally encrypted at rest and in transit, confidential computing protects your data while it's being processed.

3.1.6 *Confidentiality* — Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [SOURCE: ISO/IEC 27000 : 2016, 2.12]

3.1.7 *Data Capture* — The action or process of gathering data for storage, communication and processing, either directly from sensors and other field devices or as it gets generated by the digitization or digitalization processes.

3.1.8 *Data Classification* — Process of organizing data by relevant categories so that it may be used and protected more efficiently. On a basic level, the classification process makes data easier to locate and retrieve. Data classification is of particular importance when it comes to risk management, compliance, and data security.

3.1.9 *Data Governance* — Collection of practices and processes which help to ensure the formal management of data assets within an organization.

3.1.10 *Data Privacy* — Rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information. [SOURCE: ISO/TS 19299 : 2015, 3.32]

3.1.11 *Data Quality* — Refers to the state of qualitative or quantitative pieces of information. There are many definitions of data quality, but data is generally considered high quality if it is "fit for its intended uses in operations, decision making and planning". Moreover, data is deemed of high quality if it correctly represents the real-world construct to which it refers.

3.1.12 *Data Transformation* — Process of converting data from one format or structure into another format or structure. It is a fundamental aspect of most data integration and data management tasks.

3.1.13 *Data Variability* — Changes in transmission rate, format or structure, semantics, or quality of datasets. [Source: ISO/IEC 20546 : 2019]

3.1.14 *Data Variety* — Range of formats, logical models, timescales, and semantics of a dataset.

NOTE — To entry: Data variety refers to irregular or heterogeneous data structures, their navigation, query, and data typing. [Source: ISO/IEC 20546 : 2019]

3.1.15 *Data Velocity* — Rate of flow at which data is created, transmitted, stored, analysed or visualised. [Source: ISO/IEC 20546 : 2019]

3.1.16 *Data Veracity* — Completeness and/or accuracy of data. [Source: ISO/IEC 20546 : 2019]

3.1.17 *Data Volatility* — Characteristic of data pertaining to the rate of change of these data over time. [Source: ISO/IEC 20546 : 2019]

3.1.18 *Data Volume* — Extent of the amount of data (*see* 3.1.5) relevant to impacting computation and storage resources and their management during data processing Note 1 to entry: Data volume becomes important in dealing with large datasets. [Source: ISO/IEC 20546 : 2019]

3.1.19 *Data Warehouse* — A system used for reporting and data analysis, and is considered a core component of business intelligence.

3.1.20 *Digital Infrastructure* — Infrastructure that is required to support various IT, communication, and Digital systems in a city or any geographical region.

3.1.21 *Digitalization* — Process of automating business operations with the use of ICT and digital technologies.

3.1.22 *Digitization* — Act of generating a digital (quantized) representation of a continuous signal. [SOURCE: ISO 20998-1 : 2006, 2.7]

3.1.23 *Discoverability* — Discoverability is the characteristic of an endpoint on the network to be found dynamically and for that endpoint to report its services and their capabilities through a query mechanism or self-advertising mechanism; whichever is suitable for the device in question. The endpoints concerned could be IoT devices, services and applications, or even users. Related discovery services allow endpoints to be located, identified and accessed according to variable criteria, such as geographic location or service type.

3.1.24 *Emergence* — Principle that entities exhibit properties which are meaningful only when attributed to the whole, not to its parts.

NOTE — To entry: These properties cannot be reduced or decomposed back down to those of any individual constituent system.

[Adapted from ISO/IEC/IEEE 21840 : 2019. (en), 3.1.3]

For BIS use only, New Delhi:2021-01-08 16:08:56

3.1.25 *Emergent Functionalities* **—** Functionalities that are not directly designed in, but which become available due to the unplanned or unanticipated interactions and interplay of a large number of existing functionalities, subsystems, components and entities.

3.1.26 *Evolutionary Development* — Process of incrementally and adaptively changing and enhancing a system to meet emerging needs.

3.1.27 *Extendable* — Ability to add to a systems capability over time, beyond what it was originally designed with.

3.1.28 *Flexibility* — Flexibility is the capability of a system, service, device or other component to provide a varied range of functionality, depending on need or context. [Source: ISO/IEC 30141 : 2018 Modified]

3.1.29 *Functional view* — Architecture view from the functional viewpoint.

[Source: ISO 14813-5 : 2020]

3.1.30 *Geographic Distribution* — Spread of a system and/or its subsystems or components across a geographically large area.

3.1.31 *Heterogeneity* — Difference arising from different descriptions of the same concept.

[Source: ISO/IEC TR 20943-5 : 2013]

3.1.32 *Infrastructure* — System of facilities, equipment and services needed for the operation of an organization, society, or a city.

[SOURCE: ISO 9000 : 2015, 3.5.2, adapted]

3.1.33 *Integrated Command and Control Center (ICCC)* — An Integrated Command and Control Centre (ICCC), as the name suggests, works as a brain for all smart solutions implemented across a city – be it a surveillance system, smart traffic management, waste management, utilities management, environmental sensors, public information system, (variable message boards, public address systems, kiosks, etc).

3.1.34 *Integrity* — Property of accuracy and completeness. [SOURCE: ISO/IEC 27000 : 2016, 2.40]

3.1.35 *Manageability* — Manageability addresses aspects of systems such as device management, network management, system management, and interface maintenance and alerts. Manageability is important to meet system requirements. Components capable of monitoring the system and changing configurations are needed for manageability of the IoT device, network and system.

[Source: ISO/IEC 30141 : 2018, adapted]

3.1.36 *Managerial Independence* — A system has managerial independence from another system, when the two system's management functions are carried out independently of each other, either by different management entities and/or by different management protocols and processes.

3.1.37 *Master Data Management* — Master data management ("MDM") is a technology-enabled discipline in which business and Information Technology ("IT") work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability of the enterprise's official shared master data assets.

3.1.38 *Metadata* — Data about data.

[SOURCE: ISO 19115 : 2003]

3.1.39 *Modularity* — Degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components.

[Source: ISO/IEC/IEEE 24765]

3.1.40 *Non-repudiability* — Attribute of capturing the source or provenance of data, which once set, cannot be removed or corrupted, without damaging the data/information itself.

3.1.41 *On-Prem* — On-premises software (commonly misstated as on-premise, and alternatively abbreviated "on-prem") is installed and runs on computers on the premises of the person or organization using the software, rather than at a remote facility such as a server farm or cloud.

3.1.42 *Openness* — Absence of barriers to allow any entity access to a system's aspects like its specifications, its interfaces, its data models, its interaction modalities, its design etc. There can be varying degrees of openness depending on what aspects are exposed to whom.

3.1.43 *Operation Independence* — A system has operational independence with respect to another system when a substantial portion of its operations doesn't depend on the other system's operations or liveness.

3.1.44 *Operational View/Business Operational View* — Perspective of business transactions limited to those aspects regarding the making of business decisions and commitments among Persons, which are needed for the description of a business transaction.

[Source: ISO/IEC 14662 : 2010]

3.1.45 *Personally Identifiable Information (PII)*

Any information:

a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains,

b) from which identification or contact information of an individual person can be derived, or

For BIS use only, New Delhi:2021-01-08 16:08:56

that is or might be directly or indirectly linked to a natural person.

[Source: ISO/IEC 29100 : 2011, 2.9, adapted]

3.1.46 *Real-time Capability* — Real-time capability is a characteristic of a system or mode of operation in which computation is performed during the actual time that an external process occurs, in order that the computation results can be used to control, monitor, or respond in a timely manner to the external process. Additionally, the system has the ability to perform an action or function, or to call a service within a specified period of time, thereby supporting deterministic operations. [Source: ISO/IEC 30141 : 2018]

3.1.47 *Reference Architecture* — Architecture description that provides a proven template solution when developing or validating an architecture for a particular solution. [Source: ISO/IEC 20924 : 2018]

3.1.48 *Reliability* — Property of consistent intended behaviour and results. [SOURCE: ISO/IEC 27000 : 2016, 2.62]

3.1.49 *Repudiation* — Ability to prove the occurrence of a claimed event or action and its originating entities. [SOURCE: ISO/IEC 27000 : 2016, 2.54]

3.1.50 *Resilience* — Ability of a system to reduce likelihood of failure, to absorb effects of such failure if it occurs and to recover quickly after failure. [Source: ISO 13824 : 2020, 3.8]

3.1.51 *Safety* — Freedom from unacceptable risk, danger or injury.

3.1.52 *Scalability* — Characteristic of a system to continue to work effectively as the size of the system, its complexity or the volume of work performed by the system is increased. [Source: ISO/IEC 30141 : 2018]

3.1.53 *Smart City* — City where improvements in quality of life, services, sustainability, inclusion and resilience are accelerated by the effective integration of digital, physical, and social systems and the transformative use of data and technology.

3.1.54 *Smart City Organization* — Entity responsible for driving the adoption of technologies to realise the smart city vision.

3.1.55 *Special Purpose Vehicle (SPV)* — Special purpose vehicle is a legal entity especially constituted to undertake a set of business processes. The SPV will plan, appraise, approve, release funds, implement, manage, operate, monitor and evaluate the Smart City development projects.'

3.1.56 *Stakeholder* — Individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations.

[Source: ISO/IEC 12207 : 2008]

3.1.57 *Technology View* — Architecture view from the technology viewpoint.

3.1.58 *Unified Digital Infrastructure* — Interconnected and integrated digital infrastructures from a collection of diverse entities and organizations, working seamlessly together to present a logically unified, digital view for the collective.

3.1.59 *Urban Local Body (ULB)* — Refers to the governing body responsible for city/town/township/ village administration such as Municipal Corporation, Municipal Council, Municipality etc.

3.1.60 *Vendor* — One who sells and/or delivers equipment and/or engineering services.

[Source: ISO 35101 : 2017(en), 3.16]

3.2 Abbreviations

Abbreviation	Full Form
UDI	Unified Digital Infrastructure
ICCC	Integrated Command and Control Center
ICT RA	Information Communication Technology Reference Architecture
GIS	Geographical Information Systems
IT	Information Technology
ICT	Information and Communication Technologies
OT	Operations Technology
SPV	Special Purpose Vehicle
RFP	Request For Proposals
SOP	Standard Operating Procedure
KPI	Key Process Indicators
IoT	Internet of Things
ULB	Urban Local Body
ERP	Enterprise Resource Planning
COTS	Commercial-off-the-shelf
AI	Artificial Intelligence
ML	Machine learning
G2X	Government to entity
ITIL	Information Technology Infrastructure Library
SWM	Solid Waste Management
ETL	Extract Transform Load

For BIS use only, New Delhi:2021-01-08 16:08:56

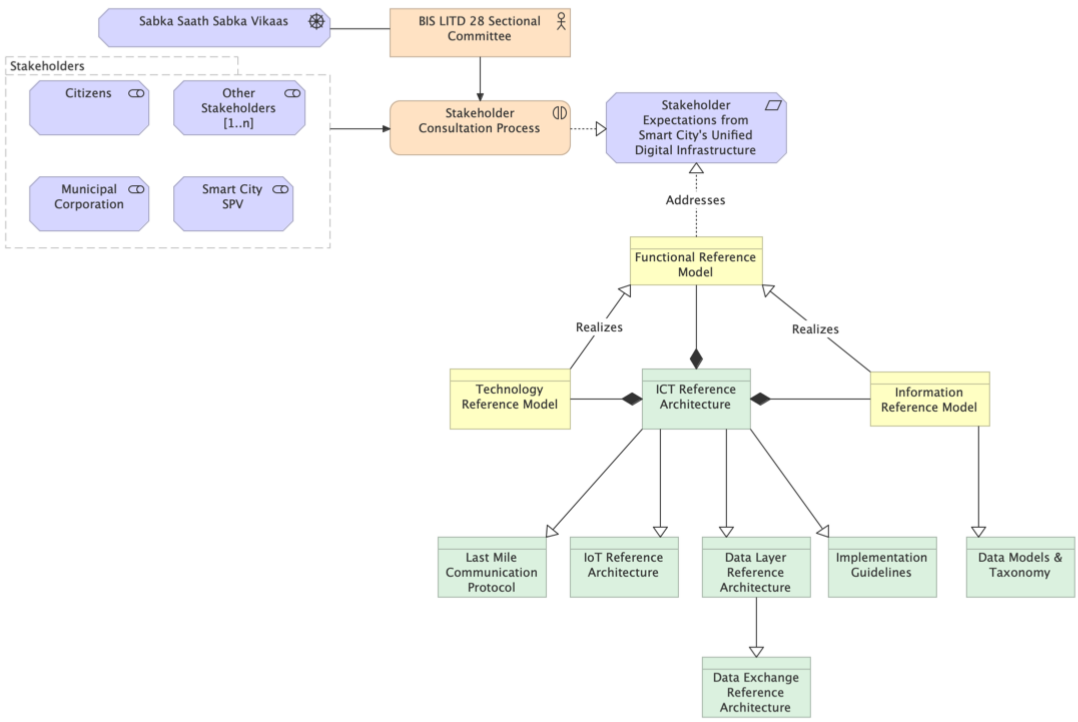


FIG. 1 ARCHITECTURE DEVELOPMENT PROCESS

4 ARCHITECTURE DEFINITION PROCESS

A Smart city is a system of systems as described in Annex A, and defining an ICT Reference Architecture for such a complex system requires a systematic approach that is articulated in Fig. 1. The figure uses the notation developed by the open group capture the process, principles and outputs of this activity.

Our development process assumes the need to work with existing legacy systems, as well as cater to development of new systems.

One of the main driving principles of our architecture definition process is "*Sabka Saath Sabka Vikaas*" that is, "*together, we develop*". In that spirit, the description of the Smart City–ICT Reference Architecture in this standard starts with capturing the stakeholder concerns (i.e. their expectations). These stakeholder concerns naturally lead to a set of functionalities that are needed to meet the expectations and these functionalities constitute the Functional Reference Model. The technology reference model and information reference models that are needed to support/realize the functionalities are derived from the functional reference model. The four while the exact concerns and functionalities may change over time, the process defined in this standard remains applicable and can be used to regularly update the reference architecture with the changing needs.

The ICT reference architecture consists of defining the following key components:

a) Conceptual model (*see* **5**);
b) Stakeholder expectations (*see* **6**);
c) Functional reference model (*see* **8**);
d) Technology reference models (*see* **9**); and
e) Information reference models (*see* **10**).

Annex B provides guidelines on how to address concerns of different stakeholders through functionalities by mapping different stakeholder concerns to one or many of the functionalities.

Annex C diagrammatically represents how different functionalities are realized by a combination of underlying components, tools, and services.

The ICT reference architecture naturally points to further areas in need of standardization and some of these are indicated in Fig. 1. These include the communication (last mile communication protocols and related standards), the data layer (data layer reference architecture, data exchange framework and related standards), the IoT related standards (IOT reference architecture), data models and taxonnomy, GIS reference rchitecture and implementation guidelines.

All the diagrams, and key elements of the architecture are made/captured in Archimate 3.1, an enterprise architecture modelling language developed by "The Open Group", and the resulting files are available online www.bis.gov.in and is a live representation of this architecture.

For BIS use only, New Delhi:2021-01-08 16:08:56

5 CONCEPTUAL MODEL

A smart city can be modelled and viewed in multiple ways and a layered or tiered view is one of the easiest to visualise and understand and one such view is given in Fig. 2. The layered view shows how the basic building blocks of a smart city fit together. For example, Domain applications and solutions, such as solid waste management, transit management, smart parking, etc., are built on top of a foundational set of ICT infrastructure and solutions. Similarly, stakeholder services, such as command and control are built on top of domain solutions whereas security and management span across layers and are present in every layer.

The Unified Digital Infrastructure ICT Reference Architecture (UDI-ICT RA) deals with the standardisation of a specific set of layers of the Smart city model. Specifically, the layers/blocks listed below:

a) ICT infrastructure and solutions;

b) GIS;

c) Stakeholder service enablement such as command and control;

d) Management; and

e) Security.

This sandard does not deal with any of the domain solutions except e-Governance in this ICT reference architecture. Separate standards exist for field operational technology (OT) devices and omain solutions.

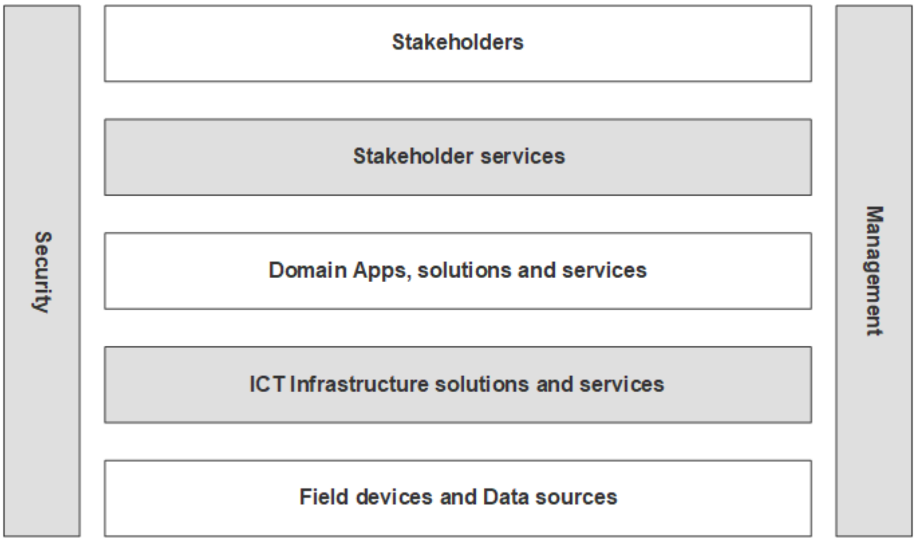


FIG. 2 SMART CITY CONCEPTUAL MODEL

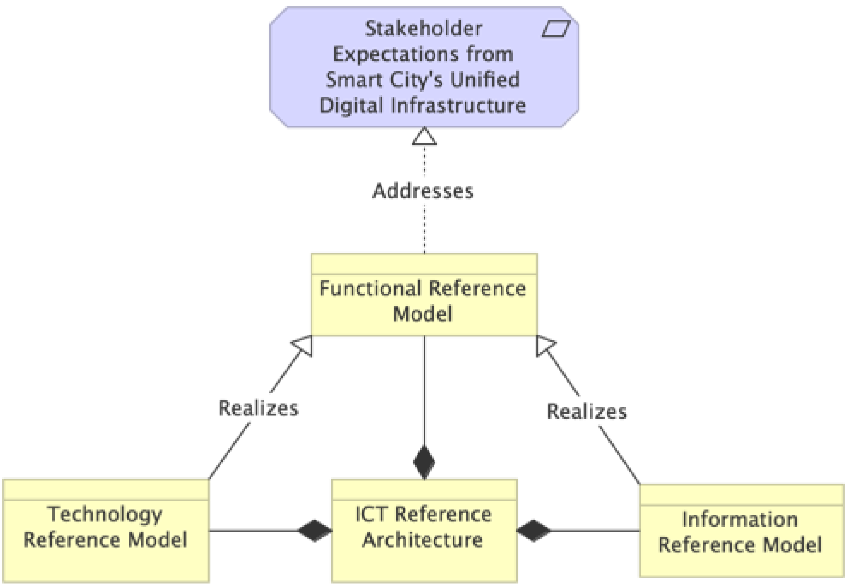


FIG. 3 ICT REFERENCE ARCHITECTURE: CONCEPTUAL MODEL

For BIS use only, New Delhi:2021-01-08 16:08:56

As depicted in Fig. 3, the ICT reference architecture comprises of three main reference models:

a) Functionalities reference model (FRM);
b) Technology reference model (TRM); and
c) Information reference model (IRM).

The FRM captures all the desired functionalities that need to be provided by the digital infrastructure for smart cities. These functionalities address (or meet) all the concerns/expectations of all the stakeholders and is the first entity that gets defined.

These functionalities are then realized by the combination of technology and data (or information) which are further elucidated in TRM and IRM, respectively.

The components of FRM and TRM are specified at a high level of abstraction, that captures their essential characteristics, yet-allows for diverse realizations, based on the needs, costs and available resources.

The IRM is also defined at an abstract level to bring out the relationships between various constituent elements like data models, data sets, taxonomies etc. as a template. Concrete instances for all of these can be defined for each domain and use case that follows this template.

6 STAKEHOLDERS AND CONCERNS

The smart city concept has opened up many opportunities by utilizing the power of data science and geographical information systems for enabling exchange of ideas, innovations, and solutions across the country that can be at the right place and time to help cities across the country solve local challenges and improve citizen service, satisfaction, liveability, and citizen involvement.

A Smart city involves many stakeholders right from the citizens, local city government, and administration all the way to the State and Central governments. The stakeholders can largely be divided into two groups namely, Internal and External.

Internal stakeholders are the municipal corporation/local city administration, the smart city SPV, utility service providers, state and central governments; and external stakeholders are the citizens, vendors, businesses, system integrators/tech companies/start-ups, academia, research institutions, etc. Each of the stakeholders has specific concerns about the services provided by the smart city. For example, on one end of the spectrum, a municipal corporation or local city administration is concerned about 360° view of the services and operations of the city, enabling close coordination between various departments and service providers to carry out smooth and seamless work activities across the city, emergency and disaster management and handling, etc. On the other side of the spectrum, academia and/or research institutions are concerned about non-discriminatory and timely access to relevant data for analysis, innovation, development activities and to provide insights. Each of these stakeholder concerns impacts different characteristics or domains of the ICT reference architecture. While the municipal corporation's concerns are more operational and informational in nature, the academia's concerns are more technological. A smart city SPV plays a major role in ensuring a fine balance between the two ends of the spectrum thus enabling better citizen service and fostering innovation yet maintaining privacy and security of valuable citizen data.

6.1 describes the stakeholders, their concerns and the relevant characteristics/areas of the ICT reference architecture that covers or addresses the concern.

NOTE — Concerns can be expectations and/or interests.

6.1 Stakeholder Roles

6.1.1 *Municipal corporation/municipal council/urban local body/municipality*

Local governing body that works for providing necessary community services like health care, educational institution, housing, transport, etc. by collecting property tax and fixed grants from the State Government.

6.1.2 *Utility Service Providers and other Departments*

Utility service providers are organisations which provide basic services like water sewerage, energy, transportation, telecommunications, police, disaster management agency etc..

6.1.3 *Smart City SPV*

The SPV will plan, appraise, approve, release funds, implement, manage, operate, monitor, and evaluate the smart city development projects. Projects involve ICT to enhance the quality and performance of utility services and community services.

6.1.4 *Citizens*

Citizens are an important aspect of smart cities. A city cannot be built smart until and unless citizens participate in the transformation. The success of smart cities relies on citizens engaging with technology solutions.

6.1.5 *System Integrators*

Systems integrator (or system integrator) is a company that specializes in bringing together component subsystems and suppliers into a whole and ensuring that those subsystems function together for the smart city.

6.1.6 *Vendors*

IT hardware vendors, hardware component makers, software vendors, business entities and channel partners

For BIS use only, New Delhi:2021-01-08 16:08:56

such as resellers and distributors who help in providing different systems to the system integrator.

6.1.7 *Business/Research Institutes*

Startups, academic institutes, and research organisations focussing on urban development and issues. Table 1 identifies all the important concerns (or expectations) of key stakeholders who will be impacted by a city's unified digital infrastructure.

Each concern should be addressed by an appropriate architectural view(s) of the UDI-ICTRA.

7 PROPERTIES

Cities being complex entities with diverse organizations having heterogeneous ICT systems, the Unified Digital Infrastructure (UDI) should embrace the system of systems perspective, which means allowing heterogeneous systems, developed and owned by different stakeholders to interact with each other in an efficient way.

To support this distributed digital ecosystem to evolve and develop in an optimal fashion, the UDI needs to have certain characteristics or properties as listed in Table 2.

Table 1 Stakeholder and Concerns

(*Clause* 6.1.7)

Sl No.	Stakeholder	Concern (Expectation)
ULB.1	Urban Local Body	Complete view of city's operations, with appropriate information also made available to various stakeholders as needed.
ULB.2		Allow for smart decision support-Data-driven decision making for service delivery and resource sustainability.
ULB.3		Allow for efficient SOP implementation and their tracking.
ULB.4		Allow for easy adoption of new SOPs.
ULB.5		Facilitate better coordination between various departments, organizations and citizens through Integration of relevant applications and workflows across diverse systems.
ULB.6		Emergency and disaster handling, management and guidelines.
ULB.7		Implement a city data policy as per existing policies and regulations for example, the data maturity assessment framework developed by the Smart Cities Mission, Govt. of India.
ULB.8		Avoid vendor lock-in at various layers. For example, while adding a new device, add a new storage server, deploy a new app/dashboard algorithm through any vendor.
ULB.9		Improve compliance with various standards and guidelines, for example, the ICCC Maturity Assessment Framework developed by Smart Cities Mission, Govt. of India.
SPV.1	Smart City SPV	Enable easy creation and rapid deployment of new ICT based services for the city and assist municipal corporation with unifying the digital infrastructure and process.
SPV.2		Allow quick and high-quality RFP specifications, that can build on and add value to existing system. Allow for archiving and sharing of various documents to enable easy knowledge dissemination and collaborations.
SPV.3		Allow easy engagement and participation of partners like academia, small businesses, citizens etc in solution development for the city.
SPV.4		Allow easy and quick onboarding/interconnection with existing systems from private or public entities
SPV.5		Effective & collaborative monitoring and management of city operations across various agencies
SPV.6		Provide tools for going towards sustainable operations, via sale of specific, value-added services.
SPV.7		Allow easy onboarding and integration of new vendors.
SPV.8		Continuous and reliable service to various stakeholders.
SPV.9		Smooth integration with systems (existing/future) of other civic bodies in the city.
SPV.10		Reliable network connectivity with options for backup and switch over to other ISPs.
SPV.11		Evaluate subsystems effectively before awarding the project.
SPV.12		Ability to provide ICT services to other urban local bodie.
SPV.13		Monetization of services for sustainable operations of smart city initiatives.
SPV.4		Data security, data sharing, data governance capabilities for effective realization of city's data policy.
SPV.15		Cataloguing, managing and enabling transport of city data as either data owner or data fiduciary with necessary permissions, security precautions and protocols.
SPV.16		Access to operational data of municipal corporation and other agencies for urban planning and scenario analysis.
SPV.17		Ownership/custodianship of smart city assets (field devices/IoT devices) and asset lifecycle.
SPV.18		Provide single window of city services to citizens.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 1 (*Continued*)

Sl No.	Stakeholder	Concern (Expectation)
C. 1	Citizens	Enable a single window to access all government services.
C. 2		Privacy preserving and informed consent for processing PII data. Also allow secure and private channels for engagement with urban local body and smart city.
C. 3		Mechanism to enhance voices of citizens - grievance, feedback and sentiment analysis.
C. 4		Multi language capabilities across platforms.
C. 5		Access to open data.
C. 6		Contribution to data (crowdsourcing).
C. 7		Traceability and predictability of government services and functions.
C. 8		Emergency and disaster behavioural guidelines.
C. 9		Equitable access to all citizens including differently abled, digitally excluded and older sections of society.
C. 10		know the realized benefits of already deployed and plans for future deployments.
VN. 1	Vendors	Allow for a standard based, well specified, neutral and reasonable RFPs to enable fair chance to win contracts.
SI. 1	System Integrators	Identification of appropriate standards to enable a compliance-based solution allowing for easy integration and deployment, and also covering data ingestion, exchange, analysis and governance.
SI. 2		Facilitate extraction and tracking of city KPIs.
SI. 3		Identification of appropriate standards for operations, management, incremental integrations and life cycle management
SI. 4		Stakeholder and project management processes and guidance and allow for phased deployment and rollout.
US. 1	Utility Services	Reports or information given back to the service providers by integrating their data and co relating with other data.
US. 2		Data security.
US. 3		Regular updating of data to facilitate better coordination between various departments.
US. 4		Ease of integration with smart city/ICCC/other stakeholders.
US. 5		Relevant analytics/reports based on data obtained from other stakeholders as well, including obtaining real-time alerts.
US. 6		Citizen service feedback.
BR. 1	Businesses/ Research Institutes	Non-discriminatory data availability for Innovation in business, start-ups and research and development activities.
SG. 1	State Government	Enable a wholistic and summary view of operations and status of all cities in the state.
SG. 2		Enforce compliance and adherence to relevant state policies and guidelines and ensure adoption of the standards compliant system.
SG. 3		Identify and rectify capacity and process related issues at the ULB level and upgrade to digitally enabled business processes as and when it is available.
SG. 4		Data availability for decision making (decision support system).
SG. 5		Coordinated emergency and disaster handling, management and guidelines. Facilitate data recovery within time bounds.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 1 (*Concluded*)

Sl No.	Stakeholder	Concern (Expectation)
CG. 1	Central Government	Enable a wholistic and summary view of operations and status of all cities in the country.
CG. 2		Track progress and compliance of central missions and schemes including fund utilization, works completion and citizen feedback.
CG. 3		Enforce national standards including data semantics in various urban domains including accounting, water, sewerage, solid waste management etc.
CG. 4		Data availability for decision making (decision support system).
CG. 5		Coordinated emergency and disaster handling, management and guidelines.
OM. 1	Operation and Maintenance Team	Documentations, maintenance contract, licenses.
VS. 1	Visitors	Ease of access to city information (maps, places of interest, hotels, restaurants, bus stops, hospitals etc).
VS. 2		Improved access to landmarks and other places of attractions (city's tourism attractions, helping tourists find the best times to visit, buy tickets in advance or give accurate directions on the go, transportation and travel).
VS. 3		Improved communication with host communities (linguistic services, bot guides, lost and found).
VS. 4		Real-time information during disasters and emergencies - (Restricted zones and ePass for restricted area, Safest route of travel to and in a city).

Table 2 Properties of UDI

(*Clause* 7)

Sl No.	Properties	Description
P. 1	Operation independence	UDI shall allow operational independence of constituent systems. Operations can be managed independently by each independent organization managing the system. Efficiencies can be achieved by autonomous organizational systems through negotiation of policies, having no compromise on quality with ascertainment of reliability and implementation viability, for achieving goals according to constraint.
P. 2	Managerial independence	UDI shall allow managerial independence of constituent systems. Component systems can be acquired by separate program offices and run by separate operation units. These organizations may not even be connected by common membership or any structure.
P. 3	Evolutionary development	UDI shall be designed to be evolvable over time thereby helping adapt to changing needs. For example, a property model that identifies the property location only through address and pin code can evolve to include latitude/longitude to provide for better location resolution.
P. 4	Geographic distribution	UDI shall allow geographic separation of constituent systems.
P. 5	New and emergent functionalities	UDI should allow new functionalities to emerge via integration of constituent systems.
P. 6	Interoperability	UDI shall enable interoperability of systems by adopting open, standards-based interfaces, protocols, common data models and communication methods at key interaction points between constituent systems.
P. 7	Openness	UDI shall be technology and vendor neutral. It should foster wider ecosystem participation and innovation through collaboration and extensibility. (Being Open also helps leverage ecosystem expertise at the time of designing and evolving the standards.)
P. 8	Extendable	UDI should be extendable thereby providing ecosystem adopters the capability to leverage these standards and innovate for their context while maintaining interoperability.
P. 9	Data privacy, security and empowerment	UDI shall provide for the mechanisms to keep the data secure (for example, mandating SSL for data in transit) and private (for example, consent based data access) while still allowing for mechanisms to exchange needed information between trusted parties.
P. 10	Non-repudiability	UDI shall provide for mechanisms to view and verify attribute trails - for example, who accessed or updated what and when-through mechanisms like digital signatures and tamper proof audit trails.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 2 (*Continued*)

Sl No.	Properties	Description
P. 11	Accessibility	UDI shall allow all stakeholders to benefit and participate via Multi-Lingual, Multi-UI, Multi-Devices, Multi-Modal methods to interact with the City's Digital Infrastructure.
P.12	Availability	UDI should make its functionalities available, accessible, and usable on demand by authorized entities. "Authorized entities" can be both human users and service components.
P.13	Confidentiality	UDI Shall support protecting the Confidentiality of information so that it is not made available or disclosed to unauthorized individuals, entities, or processes.
P. 14	Integrity	UDI Shall protect the integrity of information
P. 15	Protection of personally identifiable information (PII)	UDI shall ensure protection of PII in compliance with the applicable legal or regulatory requirements in the applicable jurisdictions.
P. 16	Reliability	UDI should be reliable. Reliability is a property of consistent, intended behaviour and results. An appropriate level of reliability in capabilities such as communication, service and data management are important to meet system requirements.
P. 17	Resilience	UDI should be resilient. Resilience is the ability of the system or its components to adapt and continue to perform their required functions flexibly in the presence of faults and failures and other ad hoc changes without loss of operation and performance level.
P. 18	Safety	UDI should be safe. Safety is the state in which the risk of harm (to persons) or damage is limited to an acceptable level. Risk is the probability of the occurrence of harm combined with the severity of that harm. Harm includes injury or damage to the health of people, or damage to property or the environment. Harm can be due to malfunction, failure, or accident. While prior traits describe the desired behaviour of the system when operating correctly, safety includes the consideration of failure modes with the intent of preventing, reducing or mitigating the potential for undesired outcomes; specifically, damage, harm or loss.
P. 19	Composability	UDI should promote composability of services and solutions. Composability is the ability to combine discrete system components into a larger component to achieve a set of goals and objectives.
P. 20	Functional and management capability separation	UDI should allow separation of functional and system management capabilities. Separation of functional and management capabilities means that the functional interfaces and capabilities of a system component, (for e.g., an IoT device) are cleanly separated from the management interfaces and capabilities of that component. This typically means that the management interface is on a different endpoint from that of the functional interface and the management capabilities are handled by different software components than the functional interfaces.
P. 21	Heterogeneity	UDI shall support a diverse set of systems and components, from multiple vendors, as well as legacy and state-of-the-art systems and components.
P. 22	Modularity	UDI should be made of modular components, whose life cycle management should be easily integrated as part of the overall management framework. Modularity is a property of components that can be combined to form larger systems of components. Modular components can be removed cleanly from a system and replaced with a module of comparable size and with similar physical and logical interfaces.
P. 23	Scalability	UDI shall be scalable. Scalability is the characteristic of a system to continue to work effectively as the size of the system, its complexity or the volume of work performed by the system is increased.
P. 24	Unique identification	UDI shall allow unique identification of all its constituent systems and components. Unique identification is the characteristic that allows for unambiguously and repeatedly associating the entities within the system with an individual name, code, symbol, or number, and to interact with the entities, or trace or control their activities, by referencing that name, code, symbol, or number. These entities include all the components of the system itself, such as software components, sensors, actuators, network components, computers and any other assets associated with the UDI.
P. 25	Well-defined components	UDI should maintain a registry of all constituent components and the associate description of their capabilities and including any associated uncertainties or limitations. Capability information includes not only information about the specific component functionality, but configuration, communication, security, reliability, and other relevant information.
P. 26	Compliance	UDI shall be compliant to all applicable rules, regulations, standards, and policies. Compliance is the characteristic of conforming to rules, such as those defined by a law, a regulation, a standard or a policy. All the constituent systems, services, components and applications can be deployed in circumstances which require adherence to a variety of laws, policies, or regulations. Such support can be inherent in the system or its components, or can require specific configuration, programming, modification or extension to ensure compliance.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 2 (*Concluded*)

Sl No.	Properties	Description
P. 27	Data characteristics–volume, velocity, veracity, variability and variety	UDI shall be able to handle the "data 5Vs" of volume, velocity, veracity, variability and variety. The data 5Vs derive from big data systems-city systems are the sources of data which is large in volume, delivered at speed across network links, whose veracity needs to be validated (for example, due to malfunctioning sensors or improper inputs), which can vary over time and can contain a wide variety of different data types from different system components.
P. 28	Discoverability	UDI shall allow discoverability of functionalities, services, data and any other relevant resources via both human and software agents. Discoverability is the characteristic of an endpoint on the network to be found dynamically and for that endpoint to report its services and their capabilities through a query mechanism or self-advertising mechanism; whichever is suitable for the system or component in question. The endpoints concerned could be IoT devices, services and applications, or even users. Related discovery services allow endpoints to be located, identified and accessed according to variable criteria, such as geographic location or service type.
P. 29	Flexibility	UDI shall be flexible. Flexibility is the capability of the system to provide a varied range of functionality, depending on need or context.
P. 30	Manageability	UDI shall be manageable. Manageability addresses aspects of systems such as device management, network management, application management, user management, system management, and interface maintenance and alerts. Manageability is important to meet system requirements. Components capable of monitoring the system and changing configurations are needed for manageability of all the systems and their constituents.
P. 31	Real-time capability	UDI shall support real-time services. Real-time capability is a characteristic of a system or mode of operation in which computation/analytics is performed during the actual time that an external process occurs, in order that the computation results can be used to control, monitor, or respond in a timely manner to the external process. Additionally, the system has the ability to perform an action or function, or to call a service within a specified period of time, thereby supporting deterministic operations.
P. 32	Service and data subscription	UDI shall allow subscription to services and data by users who can be human or software agents. The subscription process can include payments, and a clear statement of any prerequisites as well as service and/or licensing terms and conditions that apply to the user.
P. 33	User Friendliness	Any components requiring human interactions will be designed in such a way that each of the constituent systems should be user friendly, efficient, effective, and easy to navigate. Navigation through the component should flow smoothly and it should be intuitive and adaptive to use.

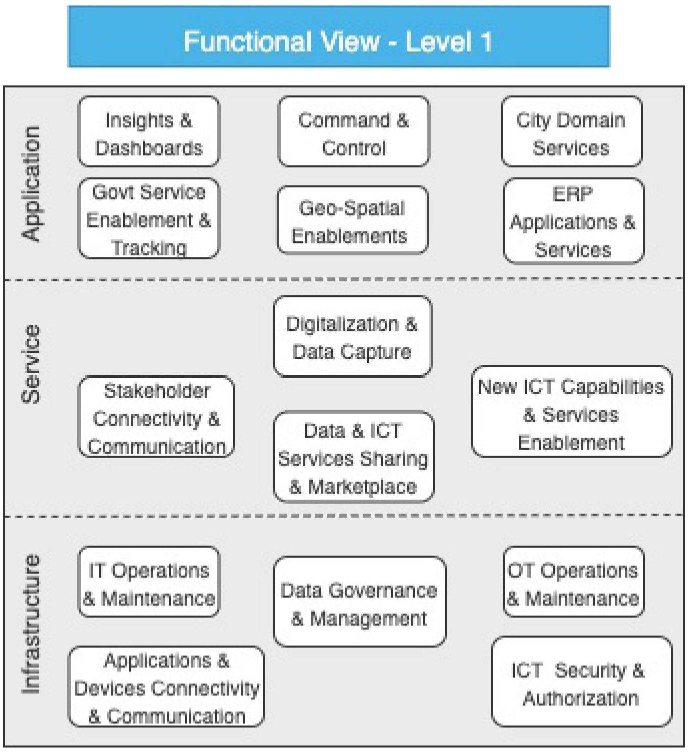


FIG. 4 FUNCTIONAL VIEW OF THE ICT RA

For BIS use only, New Delhi:2021-01-08 16:08:56

8 FUNCTIONAL REFERENCE MODEL

Figure 4 captures in an abstract form, all the key functionalities of a smart city ICT system for it to meet the expectations/concerns of all the stakeholders.

There is no implication of the implementations of these functionalities.

For a complex entity as a city, it is highly likely that these functionalities will have to be orchestrated across multiple applications, spread across diverse individual systems, managed by different entities.

These functionalities are grouped into three categories as defined as below:

a) *Application* — These functionalities are required to meet everyday city administration's business operations. Applications fall under the following 4 categories: Government to Citizen (G2C) engagement, City Operations, Inter and Intra Department processes automation and Decision Support Systems. Each block is expanded to level 2 where individual constituents of these blocks will be explained in brief.

b) *Service* — These functionalities are independent of any specific business process but are required to enable many of the application/business process functionalities.

c) *Infrastructure* — These functionalities provide core capabilities and services to maintain, manage and run the ICT infrastructure through which all ICT functionalities are enabled.

Table 3 lists out all the primary functionalities and a brief description of the functionalities that are needed to meet the stakeholder concerns.

Table 3 Primary Functionalities

(*Clause* 8)

Sl No.	Functionality	Description
F. 1	Insights and dashboards	Insights and dashboards will enable stakeholders to get a holistic view of the city's operations and status. In addition, they will enable data driven and evidence-based decision making and planning.
F. 2	Command and control	This functionality will help the City's Administrators to carry out the city's operation both during normal times as well as during emergencies, in a holistic and integrated manner, should be available 24/7 and be accessible by all the relevant stakeholders.
F. 3	City domain services	A multitude of city specific application services in the domains such as traffic management, waste management, parking, health, etc. will be supported via these functionalities.
F. 4	Govt. services enablement and tracking	The core functionalities of City's Administration to deliver all G2X services (G2G, G2B, G2C) in a measurable way.
F. 5	ERP applications and services	Enterprise resource planning and management via a suite of applications and services to fulfil City Government's operations like procurement and inventory management, asset management, project management, HR and payroll and financial management on a single, integrated, real time platform.
F .6	Stakeholder connectivity and communication	Tools and services to connect with all the stakeholders. Examples include web portals, web-apps, mobile apps, chatbots, public messaging systems, social media, email, SMS etc.
F. 7	Data capture and digitalization	Data capture refers to the tasks for capturing physical signals electronically via sensors (through process of digitization) or data from people via forms or other human-digital interaction means and finally data from within digital systems themselves. Digitalization refers to onboarding of physical documents (based on paper) into the digital domain via scanning. In addition, it includes capture of existing business processes into the digital domain to enable better tracking and management of these.
F. 8	Data and ICT cervices sharing and marketplace	These functionalities will enable creation of data collaborations amongst various stakeholders, as well as enable release of non-sensitive and non-PII data from the government departments under Govt's Open Data Policy. These will include creation and maintenance of data and service catalogs, which will be machine discoverable. In addition, certain data could be made available for commercial use under a marketplace. Moreover, the City's ICT infrastructure could also provide other services to various stakeholders (for example, ERP services and ICT services to smaller departments, etc.).
F. 9	New ICT services and capabilities enablement	ICT tools to provision, integrate and orchestrate new services on the City's digital infrastructure to enable it to grow and adapt to new requirements and concerns. These should be user-friendly to use by the technical teams of the concerned departments.
F. 10	IT operations and management	Sets of tools and services to help maintain, administer and manage the IT infrastructure and all the services running on it. Provide support for creating and managing service logs to derive various KPIs and metrics.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 3 (*Concluded*)

Sl No.	Functionality	Description
F. 11	Data governance and management	Capabilities to realize data governance in terms of data transformations and cleaning, data quality checks and improvements, data validation and audit, data security and classification, adherence to data privacy laws, meta-data creation and management etc. Capabilities to realize data management in terms of data retention and archiving, data storage, backup and redundancy management, master data management, data querying and analytics orchestrations.
F. 12	OT operations and management	Capabilities to manage the provisioning, operations and maintenance of ICT hardware, system software and firmware, their configuration, security provisioning and patches, device life cycle management etc.
F. 13	Applications and device connectivity and communications	Capabilities to provide connectivity and communication amongst applications and devices for achieving unification in the digital infrastructure. These will be realised through enterprise service busses, messaging middlewares etc. at application level and wireless and wired communication networks at the device level.
F. 14	ICT security and authorization	ICT security shall encompass all the systems and components and include devices, data, software, network elements, computers and storage elements. Authorization encompasses the ability of service and data owners to define access policies and authorize access privileges to consumers. Consumers can be human or software agents.
F. 15	Geo-spatial enablements	Capabilities to aid in Geo-Spatial enabled planning, design and operations for various urban and city activities.

Each of the above functionalities are composed of various sub-functionalities and are explained in **8.1** to **8.15**.

8.1. Insights and Dashboards

8.1.1 *Dashboards and Visualizations*

Data rendered in its appropriate context, leading to a meaningful interpretation, is of great value to all the stakeholders. This rendering of data along with its context can be done in response to a specific query or could be a continuous ongoing process. Such information can be rendered as text, images or graphs, audio or video. ICT Platforms and tools should enable each stakeholder to access information of use to them, customised as per their preferences. It is critical to ensure that there is equity and fairness to access and render information, no matter the stakeholders' constraints or background or abilities. Advanced AI and ML technologies coupled with new and emerging user interfaces, should be used to make the access and rendering of information in as natural and easy way as possible.

8.1.2 *Insights and Predictive Analytics*

Extracting deeper insights from information will involve an active process of playing with data and looking at it in various forms, with various contexts. The ICT framework should make it easy to develop processes and capabilities to allow various kinds of explorations with data, in pursuit of insights as well as predictions. These predictions could also be connected with the notification system to raise alarms so that preventive actions can be taken by the supervisors. Generation of insights and predictions should be doable by a professional analytics team or by an individual stakeholder, using both current as well as historical data. Access to large volumes of data will be important to create sophisticated machine learning based models. The ICT framework should enable easy creation and sharing of such models, as well as allow such models to be created in a federated way without compromising privacy and confidentiality.

8.2 Command and Control

The basic functions of command and control can be summarized as[1]:

a) Establishing intent;
b) Determining roles, responsibilities and relationships;
c) Establishing rules and constraints;
d) Monitoring and assessing the situation and progress;
e) Inspiring, motivating and engendering trust;
f) Training and education; and
g) Provisioning of resources.

UDI will play an important role to enable and support these functionalities.

These functionalities are fractal in nature that is, they are applicable across different organizations as well as across different units within the same organization. Hence, a key requirement for the UDI is the facilitation of collaboration, cooperation and coordination via sharing of data, information, insights and knowledge across various entities.

[1] Understanding Command and Control, Alberts, D.S., and Hayes, R. E., 2006, CCRP Publication Series

For BIS use only, New Delhi:2021-01-08 16:08:56

The functionalities listed above are also in play across three-time scales:

1) *Immediate Term or Reactive*

   In this mode, the business processes that are already put in place, are live and in operation. As new data or information flows in, appropriate workflows and actions are carried forward to further the objectives of the processes. These workflows are usually activated by the arrival of new data, leading to alerts and triggering of the appropriate business processes. ICT can play an enabling role in automating many aspects of these flows to ensure smooth and efficient realization of these business processes.

2) *Medium Term or Tactical*

   Data when rendered in the appropriate context, leads to creation of information that can be interpreted by the human agents. Rendering of information can be textual or visual and will allow the human agents to make sense of the various ongoing processes. This will allow them to fine tune, adapt and improve existing processes as well as add new processes or remove stale processes.

3) *Long Term or Strategic*

   Analysis of data and information to draw insights will lead to better understanding and planning for long term systemic changes.

8.2.1 *Establishing Intent*

The articulation of mission goals and objectives and its codification into measurable outputs and outcomes are a key requirement for any organization. These goals and objectives effectively translate into "commands or goals" for the enterprise to achieve. Synchronization and synergizing of mission goals across different inter-related entities in the city will lead to more effective outcomes and outputs for the entire ecosystem. Effective communication of these goals and objectives to all the participating stakeholders will lead to more efficient implementations. Tools and mechanisms like collaboration platforms, messaging platforms and document management and sharing platforms can go a long way in easing the implementation of these functionalities.

8.2.2 *Determining Roles, Responsibilities and Relationships*

Planning, defining and articulating the roles, responsibilities, and relationships of the various participating entities is an essential requirement to achieve the mission goals for the enterprise. This includes:

a) Streamlining and standardization of operations; and

b) Interdepartmental collaboration.

ICT tools can help codify, constrain and regulate these interactions via standard operating procedures (SOPs), as per the mission requirements.

With multiple entities, across different organizations, involved in working collaboratively to achieve mission goals, it becomes important to have automated frameworks and tools that can help to facilitate and regulate the flow of information and interactions.

Many of the mission goals need to be achieved in a distributed, collaborative manner as opposed to a hierarchical approach. Examples like, public health, cleanliness etc will need widespread citizen participation and hence, it is even more important to have appropriate mechanisms to help communicate, define, inspire, encourage, support, and monitor such activities.

Such mechanisms will also play an important role in Planning, through aids for Predictive modelling, Simulations and exploration of What-If scenarios.

8.2.3 *Establishing and Enforcing Rules and Constraints*

The laws of the land, contractual obligations, policies and other moral and implementation constraints (like health, environment, employee morale etc.) will lead to rules of engagement and operations. ICT can play an important role in codifying as well as enforcing adherence to these, via incorporation into standard operating procedures, data logging for audits and analytics driven alerts to inform when constraints or rules are close to being violated.

8.2.4 *Monitoring and Assessing the Situation and Progress*

Getting continuous and timely data that can lead to a holistic view of the ongoing mission projects and operations is critical to ensure that the eventual outcomes and outputs are successfully realized. An integrated command and control centre (ICCC) play an extremely important role in facilitating this. Data collection from various sources and its rendering in meaningful ways via dashboards and alerts, and its contextualization with overlays from different inter-related data sources, will allow a complete situation awareness, and will make it easier to adapt and modify to meet evolving needs and changing scenarios.

8.2.5 *Inspiring, Motivating and Engendering Trust*

Many of the city's operations involve voluntary participation from various stakeholders. Inspiring and motivating them to participate is an important and challenging task. Transparent processes, wide spread data sharing, open systems are some of the ways trust can be built. ICT will play a major role in the latter (via open data, standards and trusted process and frameworks). Additionally, modern ICT communication and collaboration platforms will allow effective communication and dialogue amongst

For BIS use only, New Delhi:2021-01-08 16:08:56

various stakeholders, including providing a "Citizen's view", thus increasing the quality and quantity of their participation.

8.2.6 *Training and Education*

Continuous training and education of all the stakeholders is essential to ensure smooth operations of all processes. ICT platforms can play a pivotal role in enabling this as once the processes are codified in a digital form, they can be easily shared across different stakeholders and cities. In addition, ICT platforms will enable easy content creation and sharing as well as knowledge sharing via online portals, forums and learning platforms.

8.2.7 *Provisioning*

Provisioning of resources is a critical task to ensure the success of any operation. ICT tools to help plan and manage this activity is essential, especially for complex operations that involve scale or involve many different stakeholders.

8.2.8 *Integrated Command and Control Centre*

An Integrated Command and Control Centre (ICCC) can act as the "nerve centre" for operations management, day-to-day exception handling and disaster management. It can also enable derivation of insights by processing complex data sets at an aggregated level to derive intelligence for improved planning and policy making. The ICCC should aggregate information across multiple applications and sensors deployed across the city, and then provide actionable information with appropriate visualization for decision makers. Such a service might also be made available to other stakeholders (for example, for smaller urban local bodies).

The ICCC should also have control capabilities of the city domain systems for cases where this is needed. It should be able to seamlessly monitor and provide command and control to these systems across any application vertical and across any application technology.

The ICCC can be configured to deliver several functionalities of interest to the various stakeholders. Examples include use cases for:

a) Utilities (like water, roads, power, sewerage, streetlights etc.); At a minimum, the ICCC can integrated key data points from these various systems and provide an integrated view of the state of these systems, including their key performance indicators. At the other end of the capability, the ICCC can also become the operational and control centre for these utilities.

b) Mobility services like public transport, traffic, public parking, etc. The ICCC can help provide various stakeholders with specific views and insights as per their requirements. For a commuter, ICCC can facilitate creation of mobility apps, by feeding them with data from diverse mobility service providers. For an urban planner, the ICCC can provide data and analytics tool to extract mobility patterns and allow them to do what-if scenario planning. For urban local body or traffic police, the ICCC can provide real time traffic situation for better congestion management.

c) Safety, surveillance and disaster management: Integrated archival and real-time views from multiple data providers (public as well as private sources), will enable entities like police and other first responders to offer better safety and disaster mitigation services.

d) Convergence, governance and interactions: ICCC can integrate convergence and integration of multiple and diverse applications including e-Governance, ERP, GIS, etc. In addition, ICCC can enable a wholistic and synergistic interactions with multiple stakeholders via different modalities like call centres, grievance cells, mobile apps, website, messaging displays, etc.

8.3 City Domain Services

A successful smart city strategy hinges on the ability for cities to collaborate and innovate across various domain areas like safety, health, transportation, utilities, buildings, sustainability and education. A few examples of domain services in a smart city are-crime detection and prevention, automated solid waste collection from homes, early disaster detection and management, leakage detection, intelligent streetlights, virtual health assistance, 24×7 water supply, 24×7 energy supply, multi-modal public transportation etc.

There are a host of solutions which are deployed across all these city domains, like facial recognition system, enterprise management system, public address system, variable message display system, smart lighting system, adaptive traffic control system, smart parking system, energy metering, water metering, etc. These domain solutions could be either IoT based, non-IoT based or a combination of both, and demonstrate complex operation and maintenance processes, mainly related to their nature, and involvement of multiple stakeholders from different disciplines and domains.

Seamless access and experience for all the consumers across all these services is needed, regardless of who or which combination of stakeholders fulfil the services. Thus, there is a need to facilitate interoperability, collaboration, coordination, orchestration and synergy across diverse participants in each of these city domains in order to improve quality of life of citizens and increase cost savings for the city. Besides the operational complexity, various smart city domain solutions have to fulfil strict quality requirements such as reliability, availability, maintainability, interoperability, security and privacy.

For BIS use only, New Delhi:2021-01-08 16:08:56

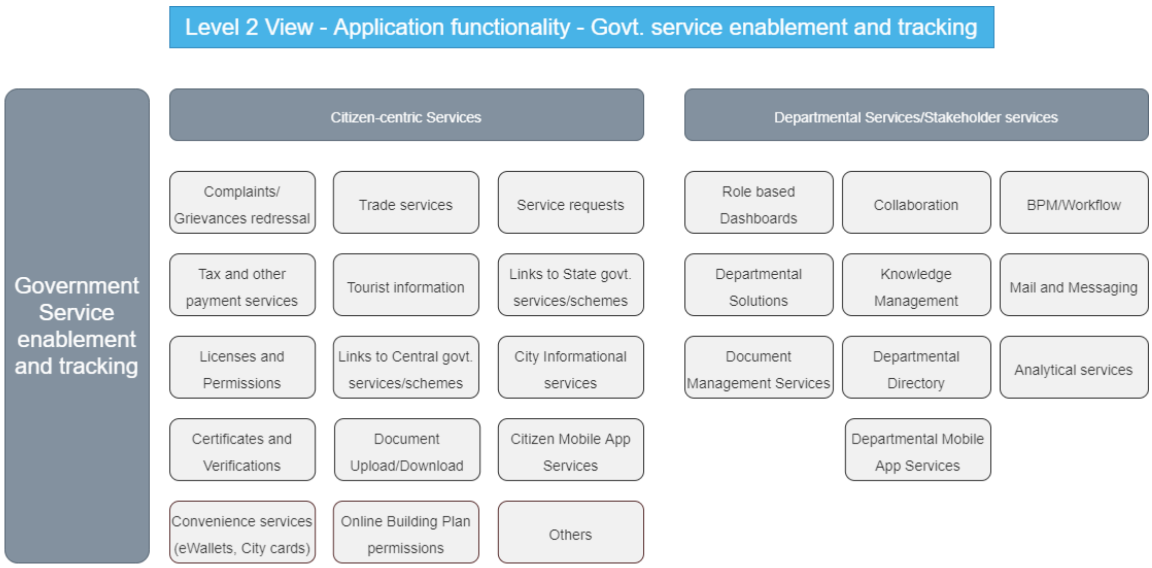


FIG. 5 APPLICATION FUNCTIONALITY GOVERNMENT SERVICE ENABLEMENT AND TRACKING-LEVEL 2 VIEW

8.4 Government Service Enablement and Tracking

Figure 5 shows level 2 view of the Application functionality government service enablement and tracking. For services provided by the government entities, UDI should provide a single logical window to the service consumer to request, access and track government services. These government services could be provided by different departments, yet a single access point to discover and consume these services will be a great benefit to all the stakeholders. Orchestration, integration, tracking and management of these services across different participating government departments, will be needed. UDI should accommodate easy onboarding of new departments, new services as well as modification and removal of services. These services could be complex workflows involving a mix of human and IT interactions.

8.5 ERP Applications and Services

City governance system comprises two broad building blocks:

a) Citizen service delivery platform (CSDP); and

b) Integrated back-office operations platform (IBOP) or ERP.

Each of these building blocks serve a unique purpose and play an important role in the transformation of the city's governance, **8.5.1** to **8.5.5** gives an overview of level 2 functionalities of ERP while Annex D describes them in detail. This block in the city governance architecture comprises 5 functionalities that are key to financial sustainability of city governments. These functionalities are:

1) Accounts, budget, investment and planning;

2) Asset, land and real estate management;

3) Project or works management;

4) Procurement and materials management, and

5) Human resource, payroll and employee self service.

All the 5 functions are truly integrated and form the backbone of the expense management for a city.

8.5.1 *Accounts, Budget, Investments and Planning*

Financial management is a key reform area in the public sector, especially in local bodies. A comprehensive, end to end financial management system would go a long way in transforming local bodies and making them sustainable. As indicated in Fig. 6, the functional architecture for Financial management system is built on 4 pillars, budgeting, financial accounting, investments and treasury and management accounting or planning. Each pillar is tightly integrated to the other to ensure a seamless flow of information across these modules. These can further be visualized via a GIS enabled dashboard for ward wise, asset wise etc. expenditures, to provide better insights to the administrators.

8.5.2 *Asset, Land and Real Estate management*

Asset, land and real estate management (*see* Fig. 7) is an often-neglected area in cities. Cities hold assets such as Lands, roads, bridges, plants and equipment, and other assets worth a large amount of money. Poor visibility and management of these assets lead to losses as well as inefficient spending. An efficient asset management system for a city will help it achieve sustainable development without putting pressure on revenue budgets. Further, it will help minimize cost, facilitate long term planning and help respond better to disaster/pandemic situations.

For BIS use only, New Delhi:2021-01-08 16:08:56

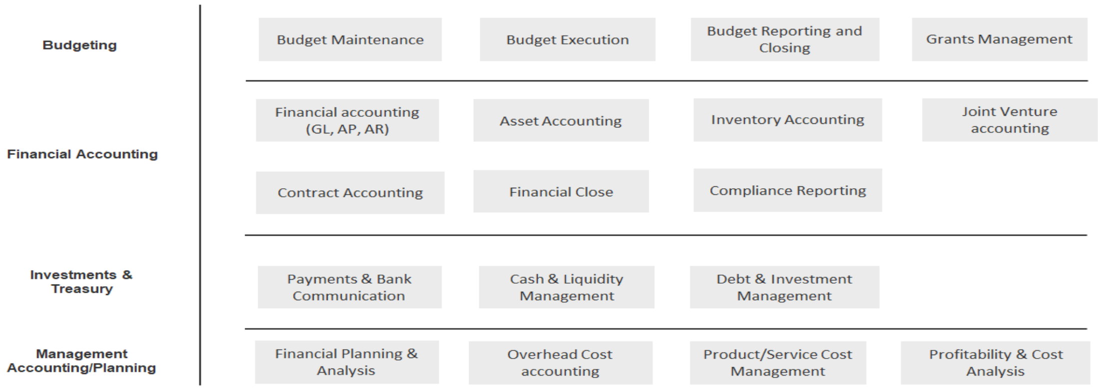


FIG. 6 ACCOUNTS, BUDGET, INVESTMENTS, PLANNING

FIG. 7 ASSETS, LAND AND REAL ESTATE MANAGEMENT

8.5.3 *Project (Works) Management*

City infrastructure development is one of the key deliverables for any city government and there's an increased focus on monitoring capital expenditures of the city. Cities are not only expected to increase their capital spend but also ensure efficiency in that spend to get maximum value out of every rupee spent. Capital project management (*see* Fig. 8) plays an important role in the day-to-day life of city engineers as it helps them keep track of the progress of each project, assess and manage associated risk, and keep a tab on the actual vs planned expenditures.

8.5.4 *Procurement and Material Management*

Transparent and efficient procurement system goes a long way in improving the financial health of the city. With right checks and balances, correct supplier information and up to date procurement records, cities can utilise this platform to save cost by procuring the right quantity and quality. Similarly, real time visibility of inventory and its movement can help reduce leakages. A strong inventory management system can have an positive impact on the organization's balance sheet and financial standing that can go a long way in improving a city's credit worthiness. Procurement and material management is depicted in Fig. 9.

8.5.5 *Human Resource, Payroll and Employee Self Service*

Human capital management (HCM) is an upcoming subject in the public sector, but its importance cannot be overstated. Something as simple as timely and correct processing of payroll can help improve employee morale and at the same time save hours of effort in accounting. Another area where HCM will play an important role is the area of skill management. The changing paradigm around us requires public sector employees to don many hats and an integrated skill assessment and management solution would help recognize individual skills and training requirements. Human resource, payroll and employee self service is depicted in Fig. 10.

For BIS use only, New Delhi:2021-01-08 16:08:56

FIG. 8 PROJECT (WORKS) MANAGEMENT

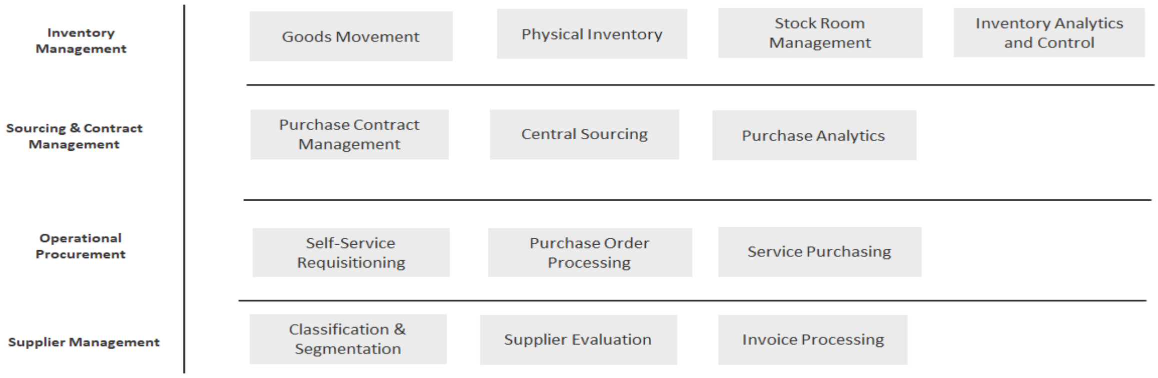


FIG. 9 PROCUREMENT AND MATERIAL MANAGEMENT

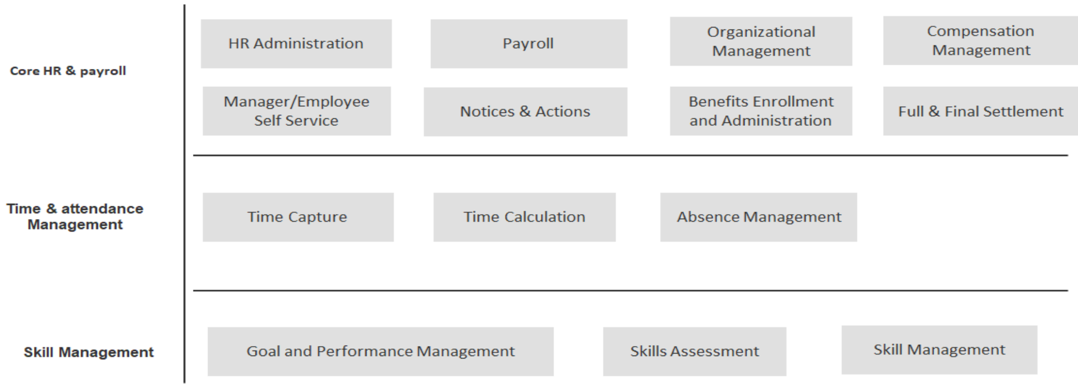


FIG. 10 HUMAN RESOURCES, PAYROLL AND EMPLOYEE SELF SERVICES

8.6 Stakeholder Connectivity and Communication

Stakeholder connectivity and communication is a critical functionality to enable an inclusive, responsive and efficient smart city. These functionalities should be integrated with the city's business processes to allow efficient delivery of government services.

8.6.1 *Broadcast, Messaging and Alerting Platforms*

Web portals, public messaging via variable messaging systems, social media platforms, SMS, chat platforms, broadcast emails are well known methods for sending out messages and alerts groups of citizens/stakeholders. A critical requirement here is establishing mechanisms to ensure authentication of the sender (to prevent fake news), message integrity (to prevent tampering), minimalistic messaging (to prevent spams), real-time ness (for critical alerts related to disaster management), multilingual and multi-modal (text, voice, video) to allow widest coverage and inclusiveness.

8.6.2 *One-to-One Communication Platforms*

Email, SMS, messaging applications, chatbots, interactive voice response system, web forms and automated speech interfaces, with multilingual capabilities, in order to provide two-way communication between individual stakeholders and

For BIS use only, New Delhi:2021-01-08 16:08:56

city administration. These tools should be integrable as part of business processes, with digital signature and other authentication technologies, to allow for easy delivery of G2X services.

8.7 Digitalization and Data Capture

Creating, managing and using data in a digital form is one of the most important features of the unified digital infrastructure. Digitalization and data capture refer to the set of functionalities that allows digital data sets to be created.

8.7.1 *Digitalization of Non-Digital Data*

A lot of data in our government offices is on paper as documents. Transferring them to a digital format will be of critical importance to realize the vision of a unified digital infrastructure. A rigorous process and SOP have to be established to allow this transfer to the digital domain to happen in a secure, non-repudiable, accurate and verifiable way, along with creation of meta-data.

8.7.2 *Data Capture by and of People*

Data capture by people refers to crowdsourcing via smartphone applications. Creating smart phone tools, processes for incentivization, sustainability and data quality checks, will enable low-cost data capture via this approach. Data capture of people refers to data about various aspects pertaining to individuals like their health etc. This data is clearly of private in nature and will need informed consent but will be important for the city from an overall administration context, public health being one example. Tools and processes to enable privacy preserving data capture, storage and analysis, consent gathering, and fiduciary responsibilities will help in proper management of data on behalf of the stakeholders. A rigorous process and SOP need to be established to allow for secure, non-repudiable, accurate, privacy preserving ways to capture, store and process this data along with its meta-data as per the country's data protection laws.

8.7.3 *Data Capture from Devices*

Data capture from devices refers to capturing data from devices like sensors and any other hardware elements like computers, switches, etc. using IoT technologies, provides another source of valuable data. Tools and processes to ensure authenticity of devices, integrity of their software and hardware, integrity and security of the communication links, security of the data and its non-repudiability and creation of meta-data are some of the important considerations.

8.7.4 *Data Capture from Applications*

All software applications either explicitly or implicitly generate data, many of which could be useful for analytics or insights. Setting up SOPs and using tools like application integration bus (or enterprise service bus), API gateways, messaging buses etc. will provide a generic way to capture data and create its meta-data from a diverse set of applications.

8.8 Data and ICT Services Sharing and Marketplace

Data collected by different entities in a smart city ecosystem, can be of a broader value to many other stakeholders. To facilitate this, the City's digital infrastructure should support the functionality of sharing of data through standardized application programming interfaces with appropriate mechanisms for access control, privacy and security. Additionally, many of the technology components that are deployed, might have excess capacity that could be made available for use by other entities, provided appropriate service interfaces are set up. Such sharing of data and services could eventually be driven through a marketplace mechanism, so that true value and costs can be discovered and shared. However, these will be governed by appropriate polices (for example, the City Data Policy), guidelines, regulations and applicable laws.

8.8.1 *Catalogues, Discovery, Reviews*

Collecting meta-data about the data sets and services, and sharing in a standard format, will allow easy search and discovery of the datasets and services and hence allow more widespread use. Standardized APIs to allow geo-spatial and attribute-based search and querying of the data sets and services will allow both humans and software to determine the presence of these. Meta-data should be rich enough to allow easy interpretation of data, its provenance, its publisher, licensing conditions, usage conditions, payment terms, and connections to other datasets. Having a review mechanism will allow consumers to rate the data sets and services, which will add more value to these from new consumer's perspectives.

8.8.2 *Access Control Policies, Authorization, Pricing and Payments*

The data or service publisher should have the ability to set appropriate access control policies to determine the consumption of the same. They should be able to determine who can consume what service for how long. The policies should be easy to set up even for a non-expert via smart phones-based apps etc. Data sets and services will be exposed only to authorised consumers as per the access control policies. This mechanism will provide a unified way to handle data of all classes (negative list, restricted, shareable, sensitive). Authorization can be gated by payments via standard payment gateways, in case the data sets have pricing requirements. More sophisticated market mechanisms for adaptive pricing, bidding etc could be supported in the future.

For BIS use only, New Delhi:2021-01-08 16:08:56

8.8.3 *Access Regulation*

Access regulation ensures data and service resources will be made available to the consumer only upon presenting valid authorisation credentials. In order to support diverse resource servers, multiple industry standards mechanisms will need to be supported through data regulation. Support for access revocation must also be provided.

8.8.4 *Data Sharing*

Data sets to be shared, shall be provided by data servers via API calls upon presentation of valid authorisation tokens.

This will allow standardized entry points for developers to access the smart city data sets under a governed manner.

Since there is a diversity of data sets (files, media, messages, records etc), having standardized APIs will allow for easy portability of applications across different smart cities.

In case of very sensitive or confidential data, data in its raw form might not be shared. Instead, either anonymized views or aggregated versions or differentially private versions might be shared. Such anonymization should be strong to prevent re-identification of PII. Alternatively, a confidential computing approach might be used to share data only in trusted computing zones, to authorised applications only. In addition, the city may provide a sandboxed data portal, where developers can build solutions and models on the exposed data.

Having the ability to share data (under privacy and access control), will enable tapping into new revenue streams.

8.8.5 *Service Delivery*

ICT services could be delivered via API gateways using one of many API forms, with REST APIs being the most common. For time critical applications, more optimized APIs (for example, grpc) could be used. Application as a service could be delivered via containers or over trusted connections to departments.

8.9 New ICT Services and Capabilities Enablement

To allow for the digital infrastructure to grow, evolve and add new capabilities via third party ecosystem, this becomes a critical functionality and may have multiple facets. Such a capability will also allow small and medium enterprises to provide value in a low-cost manner. Different components in the "New ICT Services and Capabilities Enablement" are described in **8.9.1** to **8.9.3**.

8.9.1 *API Gateways*

API gateways will allow access to APIs of the various services (especially the infrastructure services) to third party applications, and hence become an essential component. These gateways shall be able to handle scale and diverse set of protocols, shall be secure and robust to failures.

8.9.2 *Application Integration*

Integration of diverse applications will be enabled by technologies/platforms like enterprise system bus or messaging buses or similar technologies and will be important to enable all the diverse applications to work in a synergistic fashion.

8.9.3 *Hybrid cloud Framework*

Many new services and applications will need to run on the compute-data platform of the smart city. Some will need to run on the edge, some in trusted enclaves, some on-prem and some on the cloud. Hybrid cloud framework should allow seamless deployment of such services across all these layers.

8.10 IT and OT Operations and Management

Information technology (IT) and operations technology (OT) operations and management plays a critical role as they are the foundational building blocks in building a smart city. While the IT operations and management function deals with all the backend IT systems of the various domain and infrastructure solutions that are implemented in a smart city, the OT operations and management function deals with the field level intelligent and non-intelligent devices, that is IoT and non-IoT devices.

While IT and OT operations and management are categorised together under operations and management functionalities, they have distinct characteristics. While IT operations and management functionalities primarily deal with the backend IT solutions, OT operations and management functions primarily deal with field devices and their administration.

Further details of the IT and OT operations and management (*see* Fig. 11) are detailed in this and next section with a brief about each functionality. The IT operations and management should follow the ITIL practices for IT services management that is focussed on aligning IT services with the needs of a smart city business requirements. Although ITIL underpins ISO/IEC 20000, the international service management standard for IT service management, there are some differences between the ISO 20000 standard and the ITIL framework.

For BIS use only, New Delhi:2021-01-08 16:08:56

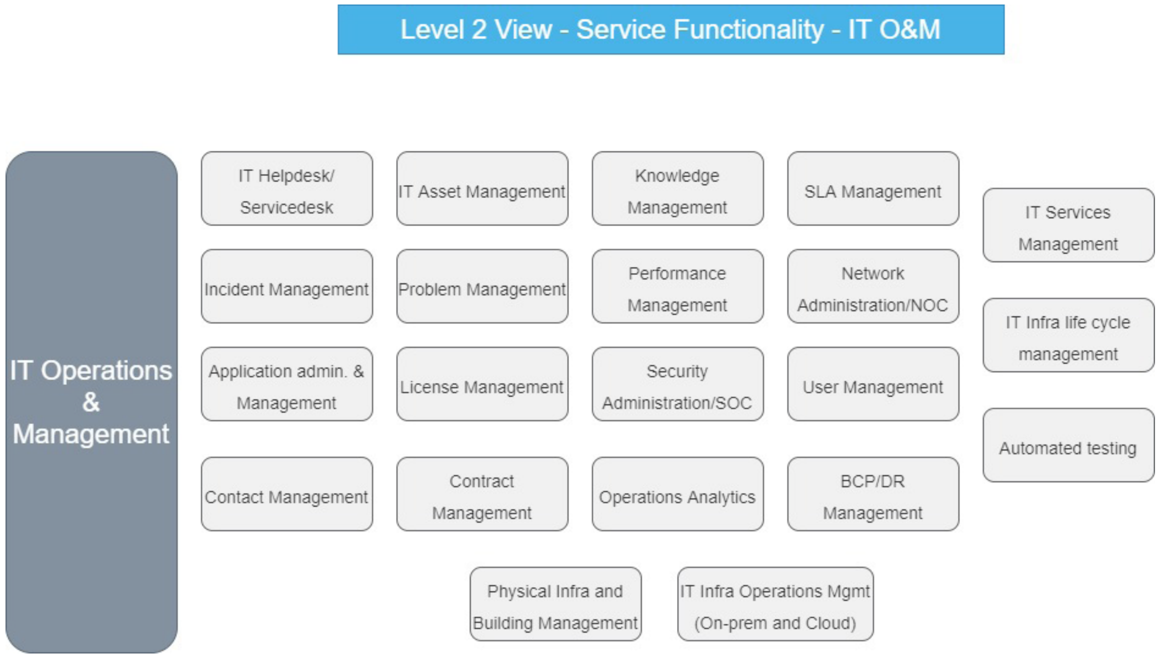


FIG. 11 IT OPERATIONS AND MANAGEMENT

Key functionalities of IT operations and management are explained in **8.10.1** to **8.10.9**.

8.10.1 *IT Helpdesk/Service Desk*

An ITIL help desk brings established best practices to the way organisations manage incidents and service requests. Help desk is the face of IT support and it mostly handles tactical operations.

Service desk is responsible for entire IT support and services which includes service request management, change management and asset management. Service desk is strategic and collaborates with other functional units to streamline support.

This functionality involves:

a) Incident logging, prioritising and ticketing;
b) Service request logging, prioritising and ticketing;
c) Case creation and workflow;
d) Case escalation;
e) Incident resolution;
f) Case closure; and
g) MIS reporting.

An organisation can deliver helpdesk/service desk functionalities through call centre/IVR, chatbot, interactive chat agents, web portals, e-mail, mobile apps, text messaging and messenger apps, such as WhatsApp.

8.10.2 *IT Asset Management*

Asset management tracks IT asset configuration, asset state and asset owner. This improves governance and helps during an asset audit. Asset lifecycle management ensures assets are tracked from installation till disposal stage along with the cost incurred at each stage. Asset ROI analysis and contract renewal become more efficient with asset management.

Asset management can also be used for non-IT assets such as field devices, however, as these devices are installed city-wide, geographically widespread and are typically operated and managed separately, it is more natural to use a solution such as GIS for managing such assets.

All physical equipment such as IT and non-IT hardware, IoT field devices and non-tangible entities like software, licenses, support subscriptions, etc. that are owned by a Smart city can be classified as assets that are to be managed.

8.10.3 *Incident Management*

Incident management aims for speedy recovery from any kind of service disruption. Incident management enables IT teams to resolve incidents quickly by configuring multiple channels and setting up automations to remove manual work. Incident management process flow includes incident logging, classification, prioritization, investigation, diagnosis, resolution and closure.

The helpdesk or the service desk is the first point of contact for an incident where it gets recorded for further action, tracking, escalation and closure. Certain incidents may result in a Service request which in turn may be serviced and tracked separately from the

For BIS use only, New Delhi:2021-01-08 16:08:56

incident. Once an incident is closed, it is generally archived in Knowledge Management System for future references. This is the post Incident activity.

8.10.4 *Application Administration and Management*

Smart cities implement both domain and IT infrastructure solutions that are quite complex and generally require careful administration to ensure they fulfill their functionality. The various application administration and management activities include:

a) Day-to-day operational activities, such as health-checks and checking logs;
b) Handling any application specific issues such as memory leaks, process/service hangs, unresponsive application, etc.;
c) User management and authorisations;
d) Applying application updates and patches;
e) Installing new versions and functionalities; and
f) Periodic business rule management and security management.

8.10.4.1 Certain solutions require specific domain knowledge on the part of the user administering or managing the solution, for example, someone managing the solid waste management (SWM) solution should have thorough knowledge of the solid waste handling and operations of the entire city. In this context, domain knowledge refers to user management within the solution and the roles of such users in a municipal corporation who handle solid waste. Availability of such domain knowledge is not a challenge as generally the solution providers possess this knowledge. He/she needs to be knowledgeable in:

a) Pickup schedules and dynamic changes to schedules;
b) Pickup routes and dynamic changes to routes;
c) Field staff availability, attendance, grievances and redressal;
d) Citizen grievances and redressal related to SWM;
e) Collection and dumping yards and related issues;
f) Monitoring and tracking of on-road SWM vehicles and handling of any incidents; and
g) Daily collection statistics and reporting.

All operations mentioned above are domain application specific administrative activities. A comprehensive solid waste management solution provides functionalities to record and track the above said activities thus enabling the administrator to run the operations smoothly and efficiently.

8.10.5 *Contact Management*

Contacting key city resources/personnel as part of operational processes and standard operating procedures during normal and emergency situations is a key aspect in a smart city. Maintaining and managing the lifecycle of such contacts and contact lists, is a key functionality required for the Smart city to perform the right operations at the right time by the right resource/person.

For example, in a Standard Operating Procedure (SOP) involving clearance of solid waste removal complaints from a citizen, a health Inspector may have to be contacted to handle the complaint and in turn, field level sanitary workers may have to be mobilised to complete the activity. Multiple resources have to be contacted in this SOP and maintaining up-to-date contact information of the right resources is important for the successful completion of the SOP.

Especially in emergency situations and the corresponding SOPs, contacting the right resources is of extreme importance.

8.10.6 *License Management*

This functionality deals with the various licenses that a Smart city needs to manage, such as software licenses, solution licenses, support licenses, licenses to operate from a specific location, etc.

8.10.7 *Performance Management*

Maintaining the optimal performance of the IT systems and solutions is key to meeting the SLA requirements and the KPIs of the smart city. Performance management directly translates into how efficiently and effectively a smart city is functioning and thus helps it improve its ranking in various pan-India surveys, such as Swachh Bharat Mission, Sustainability Index, Liveability Index, etc.

8.10.8 *IT Infra Operations Management (On-prem and Cloud)*

A smart city may deploy IT solutions either on-premise in a CAPEX model (build, own, operate) or in an OPEX model by taking IT services from a Cloud Service Provider (CSP). This functionality deals with how a smart city should manage the IT infrastructure deployed on premises, the cloud, its operations and their lifecycle. On-premises IT infrastructure management is handled by own teams of the Smart city or by a contracted vendor and this team is responsible for designing the services they will render to the user community along with the turnaround time and SLAs.

On the other hand, a CSP provides a bouquet of services with a varied level of facilities, turnaround time and SLA. Depending on the class of services that the smart city has opted for, the Smart city IT staff will have varied levels of access to the IT infrastructure.

Premium class of CSP services may allow the Smart city to fully administer and manage the entire IT infrastructure as though it is deployed on-premise, such as dynamically increasing or decreasing resources like

For BIS use only, New Delhi:2021-01-08 16:08:56

CPU cores, RAM, storage space, networking, etc., as required by the Smart city, with full administrative privileges. This enables the smart city complete control over the IT infrastructure as though it is deployed at their premises. The turnaround time for any service request will be in minutes to hours.

Whereas a basic class of CSP services may not provide any dynamic resource changes and all resource increments or decrements required by the Smart city has to be performed by raising a service request with the CSP that has a higher turnaround time running of a few hours to days.

Cloud orchestration is another critical component of cloud operations management which enables a Smart city to provision and distribute workloads across private, public cloud and on-premise ICT infrastructure, through well-defined workflows governed by security and placement policies.

If a smart city organisation decides to use the services of a CSP instead of on-premise IT infrastructure, cloud operations management plays a very important role.

8.10.9 *Operations Analytics*

Operational analytics is the process of using data analysis and business intelligence to improve efficiency and to streamline daily operations in real time and is a subset of business analytics. As such, operational analytics is much better suited to large organizations than small businesses, at least for now.

It helps in faster decision making, enhanced customer experience and increased productivity for Smart cities. Organisations can see the inefficiencies that exist in their workflows and accordingly, change their processes to streamline operations.

For example, a smart city may run analytics and realise that an SOP related to handling solid waste management is too cumbersome and inefficient and may result in automating the entire SOP. Similarly, in city administration, it may help improve the operational processes of the city government or the municipal corporation thus bringing in efficiency and improved citizen satisfaction.

8.11 OT Operations and Management

Many of the functionalities in OT operations and management may not involve any IT solution at the backend and are more of an organisational process-oriented functionalities. The key OT operations and management functionalities depicted in Fig. 12 and are briefly explained in **8.11.1** to **8.11.6**.

8.11.1 *Field Device Life Cycle Management*

Field devices that are installed across the city, may be smart IoT devices with various operational capabilities, non-IoT devices or even dumb devices. They are installed across the city and the sheer number of devices may be overwhelming for the Smart city organisation to manage and maintain them. Every field device is an important source of crucial data about some parameters of the city and so needs to be carefully administered.

Field device lifecycle includes the following important sub functionalities:

a) New device installation;
b) Device configuration;
c) Device calibration based on the geographical and other local conditions of the city;
d) Replacement of faulty, broken or stolen devices; and
e) Recycling of completely broken or obsolete devices in an environmentally safe manner.

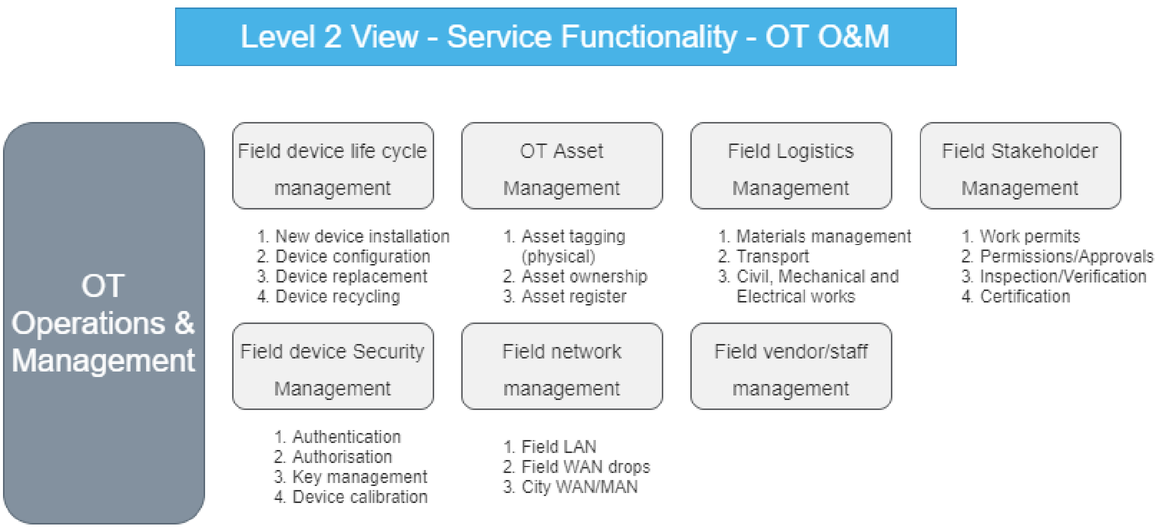


Fig. 12 OT Operations and Management

For BIS use only, New Delhi:2021-01-08 16:08:56

Smart cities may implement sophisticated backend IT solutions for field device lifecycle management or may carry this out manually through a well-defined business process. To carry out field device lifecycle management, there are software tools available which can be employed. In either case, it is an important functionality that a Smart city organisation should focus on.

8.11.2 *OT Asset Management*

Every IT or non-IT field device is a public asset that should be protected and managed by the city administration. For easy management, every such device should be easily identifiable through a well-defined asset tagging mechanism. These assets should be maintained in an asset registry using the asset tag as the key. The sub functionalities are:

a) Physical asset tagging;
b) Identifying asset ownership and custodian; and
c) Maintaining the assets in a register.

A smart city may maintain these assets in a sophisticated register such as a GIS solution or a different asset management solution, with the asset tag as the key. The asset register maintains the entire lifecycle of the asset right from its procurement, installation, maintenance to disposal of a device. The IoT Reference Architecture deals in detail with certain management components such as field device security management. Refer the IoT Reference Architecture for more information.

8.11.3 *Field Stakeholder Management*

Field device implementation in a smart city is a complicated process that may require involvement of multiple stakeholders right from city municipal corporation, state government entities and even central government entities for work permits, approvals or permissions to carry out the field work, inspection/verification for completed work and certification from relevant authorities. Involvement and managing the stakeholders at the right time will ensure that the field work activity and the implementation schedule is not impacted. As involving and obtaining necessary permissions from the relevant authorities is a time taking process, Smart city organisations should involve the stakeholders right at the start of the implementation and every stage where it is required. This is a process-oriented functionality and not a functionality that involves a backend IT solution.

8.11.4 *Field Logistics Management*

Field logistics management is another functionality that involves an organisational process more than a backend IT solution and is closely linked to the stakeholder management. Field device implementation is a complicated and a human resource intensive activity that requires skilled personnel. It involves:

a) Material management for field device installations;
b) Transportation of materials required for field device installations; and
c) Civil, mechanical and electrical works.

Each of the above-mentioned activities require supply of various materials and managing the logistics for those materials. For some of the activities, smart city may have to supply and manage the required materials, such as construction materials, electrical cables, installation panels, switches, etc. and manage the logistics (storage and transportation) of such materials.

Another important aspect of this functionality is availability and contracting of skilled resources for field work and installations which may require liaising with approved human resource service providers or contractors.

Many of these activities also require involvement of right stakeholders for inspections, verifications and certification at various stages of the installation activity. For example, the city municipal corporation's electrical department or the state electrical transmission and distribution company involvement is required to provide power supply to the field devices at the time of installation and the civil engineering department to supervise and certify the foundations laid and the civil works.

8.11.5 *Field Network Management*

Many of the field devices are sophisticated IoT devices that are capable of communicating using TCP/IP network protocol over standard Ethernet interfaces. Some even provide multiple such interfaces and dedicated management interfaces also. Today most devices, such as cameras and sensors are capable of web based interfaces for operations and management. Moreover, certain IoT devices provide edge computing capabilities for taking immediate action when an event occurs and report them to the backend IT solution at the data centre. For example, intelligent cameras can detect lost vehicles by reading the number plate and reporting when such vehicles come into view. Similarly, cameras can also detect unidentified objects. In all such cases, edge level computing capability is required and is provided as part of the IoT device itself. All such devices require interconnection and communication with the backend IT solution over the network. In a given city location, different types of smart devices with such capabilities are installed. This necessitates establishing a "mini" local area network (LAN) at that location connecting all these devices with an Ethernet switch cum router.

Each such location in the city forms a mini-LAN and so requires proper IP address allocation, distribution and management. In addition, for the backend IT solution communication, these "mini" island LANs established across the city have to be connected over a Wide Area

For BIS use only, New Delhi:2021-01-08 16:08:56

Network (WAN) through a Network Service Provider (NSP) or the city's own fibre network. Thus, the field network management involves:

a) Field LAN management;
b) Field IP management (allocation, distribution and maintenance);
c) City WAN through a network service provider; and
d) City fibre network (fibre network across the entire city owned by the city).

Those cities which do not have their own fibre network typically use the services of a network service provider for city-wide communication.

8.11.6 *Field Security Management*

As the field devices are smart IoT devices with edge computing capabilities that are capable of communicating over standard Internet protocols, they are also susceptible to cyber-attacks and hacks. Moreover, as these devices are installed in public places, they are also prone to theft, unauthorised replacement or tampering. One field IoT device in the hands of a cyber attacker is sufficient to create chaos or panic across the entire city.

Ensuring that the devices installed are genuine running the intended firmware, not compromised and the data they transmit is correct and can be relied upon is extremely critical for city stakeholders. Citizen life changing decisions are taken based on that data and it has to be safely and securely handled.

The field device security management involves the following [further details are available in IOT Reference Architecture (under preparation)]:

a) Authentication of devices to ensure that they are genuine devices and not impersonated or replaced ones;
b) Authorisation of who or what can utilise the data generated/transmitted;
c) Management of security keys that are exchanged between the field IoT devices and the backend IT solution;
d) Calibration of the device to suit the geographical and local conditions of the city and that it has not been compromised;
e) Ensuring no rogue devices are in the network;
f) Ensuring that the devices run authentic and secure firmware and not a compromised one; and
g) Device firmware updates and upgrades are carried out in a secure manner.

8.12 Data Governance and Management

Data being smart city's most valuable asset, the data governance and management architecture would need to be designed with "big data" in mind to be able to handle volume, velocity, variety, veracity and value of smart city data. IS 18002 (under development), would have the capabilities given in Table 4.

Table 4 The Data Layer Reference Architecture Capabilities

(*Clause* 8.12)

Capability	Functionality	Functionality Description
Data quality	Data cleansing	Maintenance of data to fit defined smart city data standard for enhanced interoperability and decision making.
	Data profiling	Systematic analysis of data to gather actionable and measurable information about its quality.
	Data traceability	Tracking of the lifecycle of data to determine and demonstrate all changes and access to the data.
	Data compliance	Ongoing processes to ensure adherence of data to both enterprise business rules, and, especially, to legal and regulatory requirements.
	Data monitoring	Routine checking and validation of data against quality control rules to ensure quality and format consistency.
Data architecture	Data pipelines	Data movement and transformation automation through data driven workflows.
	Architecture patterns	Facilitation and optimization of future big data architecture decision making.
	Data modelling	Creation of data models that capture business requirements and present them in a structured way.
Master data management	Data taxonomy	Classification of data within the smart city platform as defined in the smart city data standard.
	Reference data management	Setting of data values and naming standards for internal and external interoperability.
	Metadata management	Definition, creation, update, migration, and dissemination of metadata throughout the smart city platform.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 4 (*Continued*)

Capability	Functionality	Functionality Description
Data governance	Data ownership	Responsibility for the creation of the data, and the enforcement of rules as per the smart city requirements.
	Data stewardship	Assignment of accountability for the management of data assets.
	Data policies management	High-level and/or detailed rules and procedures that the smart city program utilizes to manage its data assets.
	Data standards management	Criteria, specifications, and rules for the definition, creation, storage and usage of data within the Smart city platform.
Big data management	Citizen data aggregation	Statistical models built using data processed from citizen smart city interactions.
	Big data storage	Storage, management and retrieval of massive amounts of data, or big data.
	Resource scheduling and management	Allocation system resources to specific running applications.
	Big data querying	Querying and scripting capabilities to simplify the use of big data.
	Data flow programming	Development and execution of workflows and tasks to process data for both batch and real-time use-cases.
	Data matching	Matching of data records from different data sources based on entity correlation.
Data warehouse	Data storage	Central repository for all or significant parts of the data that the smart city platform's systems will collect.
	Data marts	Correlation of diverse data streams to provide insights and trigger complex events.
	Repetitive Queries	Standardization of queries that are likely to be executed repeatedly in the future.
	Data Loading	Support for the ingestion of streaming data as well as the ability to perform continuous updates for read optimization.
Data processing	Batching	Execution of a series of programs without manual intervention on a scheduled basis.
	Streaming	Presentation of data that is being received continuously to analytics engines and dashboards.
Data transformation	ETL/ELT management	Enablement of database management processes for both traditional data warehousing as well as data lakes.
	Data aggregation	Allowing data coming from multiple sources to be filtered, correlated and aggregated before being stored.
	Parsing data management	Analysis of data to enable reading from structured and unstructured data sources.
Analytics modelling	Model building	Analysis and generation of mathematical representations of the system and its services, including the statistical models used to understand behaviours and patterns.
	Model deployment	Deployment of models in an automated fashion, without the need of a human intervention in moving code or operate the target machine where the code will run.
	Model validation	Use of various measures of statistical validity to determine data or model problems.
	Big data algorithms	Design and development of algorithms to access large amounts of data from large, cloud-based data centres through queries and derive streaming and real-time analysis from them.
	Machine learning	Automatic development of models based on training data as well as back-propagation, or feedback loops enabling the ability to test and retrain the model while processing production data.
	Statistical learning	Prediction of business metrics and variables for the future based on historic data.
Data discovery and mining	Exploratory data analysis	Analysis of data sets through visual and graphical methods to summarize their main characteristics.
	Workflow automation	Development and management of workflows to conduct analytics on data.
	Component registry management	Registry of information for reusable components of many types, which are used to build, document and test data mining tools.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 4 (*Concluded*)

Capability	Functionality	Functionality Description
Data integration and interoperability	Format translation	Translation of internal service and data formats for external platform compatibility and consumption.
	Protocol translation	Translation of internal protocols for external platform compatibility and consumption (for example, SOAP to REST).
Data exchange	Open data management	Management and accessibility of open datasets in useable formats and enablement of query generation on these datasets.
	Data visualization	Manipulation and placement of data in a visual context such as infographics, dials and gauges, geographic maps and charts.
	Dashboarding	Integration of information from multiple components into a unified display to facilitate development.
	Data sandbox environment	Isolation of computing environment in which a program or file can be executed without affecting the production environment of the services.
Data protection	Data access control	Selective restriction of access to data based on the classification of data or the authorization level of the subject trying to gain access.
	Data classification	Categorization of data to ensure efficient and effective use in line with Smart city policy and standards.
	Data retention	Ensuring availability of relevant information for a defined duration for its future reference or use.

Additionally, city data governance processes for managing smart city data needs to be put in place. These tasks can be achieved using a variety of tools and applications and are built on key data principles discussed in [Data Layer Reference Architecture (under preparation).

Whilst there are many new international standards under development for data management and governance in smart cities, following standards are suggested as a reference and can be enabled using a variety of tools and applications:

a) ISO/TS 8000 Data Quality

b) ISO/IEC DIS 20547-4(en) Information technology — Big data reference architecture

  1) Part 1 : Framework and application process
  2) Part 2 : Use cases and derived requirements
  3) Part 3 : Reference architecture
  4) Part 4 : Security and privacy
  5) Part 5 : Standards roadmap

c) ISO/IEC DIS 20546 : 2019 (en) Information technology — Big data Overview & Vocabulary

d) ISO/IEC 11179 Information Technology — Metadata registries (MDR).

e) ISO 15000 Electronic Business Extensible Markup Language (ebXML)

f) ISO/IEC 20802-1 : 2016 Open Data Protocol (OData)

  1) ISO 20802-1 Part 1: Core
  2) ISO 20802-1 Part 2: URL Conventions Plus Errata 02
  3) ISO 20802-1 Part 3: Common Schema Definition Language (CSDL) Plus Errata 02
  4) ISO 20802-2 Part 1: JSON File Format

g) ISO/IEC 29161 Data structure — Unique identification for the Internet of Things

h) ISO/IEC 30182 : 2017 Smart city concept model — Guidance for establishing a model for data interoperability

j) ISO/IEC 30182 Smart City Concept Model — Guidance for establishing a model for data interoperability

k) Linked Data from W3C

8.13 Applications and Devices Connectivity and Communication

Interconnectivity of applications, software services as well as IoT devices, in a way that they can exchange information as well as provide ICT services will be essential to allow for emergence of new capabilities. Solution providers will be able to compose new solutions and enrich the overall utility of the ICT systems. This interconnectivity should be governed by open standards, interfaces, protocols and common data models, so that it becomes easy for multi-vendor integration. At the same time, support for advanced security features, authentication mechanisms and authorization capabilities will allow multiple independent entities and departments to enable their ICT systems to participate in this collaboration, without fear of losing data or of getting hacked.

For BIS use only, New Delhi:2021-01-08 16:08:56

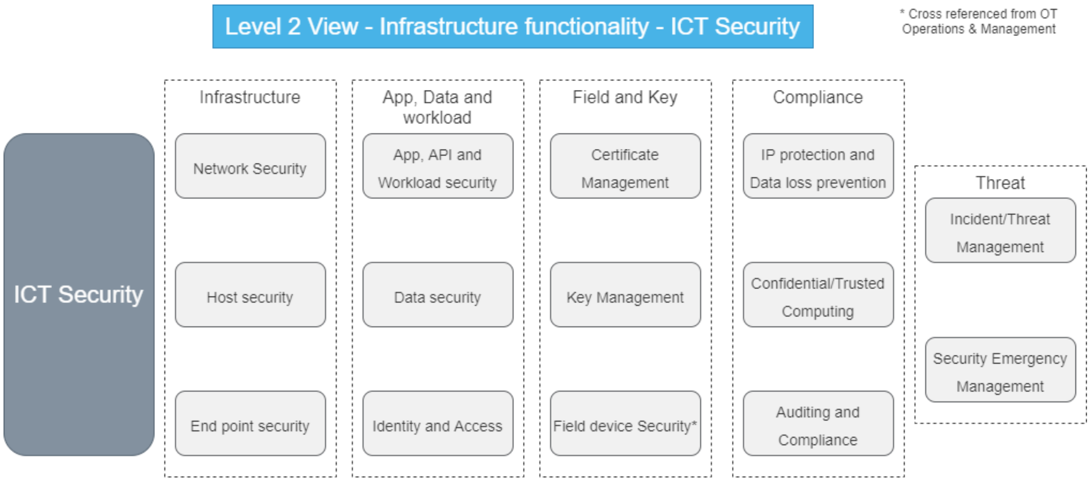


FIG. 13 ICT SECURITY AND AUTHORISATION

8.14 ICT Security and Authorization

Information security and infrastructure security plays a very critical role in protecting the Smart city physical assets such as field IoT devices, IT infrastructure and logical assets, such as field data and citizen data. ICT security covers all layers, such as infrastructure, data, integration, services and applications. The second level functionalities of ICT security and authorisation are given in Fig. 13.

Many International standards exist for covering the functionalities, such as ISO/IEC 27001 and 27002, NIST, ANSI/ISA 62443, etc. and numerous best practices exist ranging from infrastructure security to application security to data security.

Some of the key functionalities within ICT security and authorization are explained in **8.14.1** to **8.14.5** in brief.

8.14.1 *Application Security*

Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities. It deals with how an application provides secure functionalities, how securely it handles data and operations without giving rise to obvious vulnerabilities that a cyber attacker can exploit and use the application for malicious activities.

Different techniques are used to expose such security vulnerabilities at different stages of an application's lifecycle such as design, development, deployment, upgrade, maintenance. An always evolving but largely consistent set of common security flaws are seen across different applications.

There are various application security standards that exist for application security and some of the important standards are listed below:

a) CERT Secure Coding
b) ISO/IEC 27034-1 : 2011 Information technology — Security techniques — Application security – Part 1: Overview and concepts
c) ISO/IEC TR 24772 : 2013 Information technology — Programming languages — Guidance to avoiding vulnerabilities in programming languages through language selection and use
d) NIST Special Publication 800-53
e) Open Web Application Security Project (https://owasp.org)
f) PCI Data Security Standard (PCI DSS)

8.14.2 *Data Security*

Smart cities deal with a large volume of data. A city with field IoT devices installed across its nook and cranny generates and processes voluminous amounts of data at a high velocity (date rate). Each and every datum is critically important piece in the information puzzle of a city and so needs to be secured and safely stored. It needs to be protected when it is being transmitted from the field IoT devices to the processing components (data in transit) as well as after it is processed and stored (data at rest). Smart cities handle varied types of data ranging from the ones that are publicly shareable, such as, temperature or humidity at a location to data items that need to be highly protected but still shareable, such as, citizen address, or mobile numbers to the ones that should never be revealed at any cost such as citizen credit card number, bank account no. or Aadhaar details.

8.14.2.1 Data security is part of the larger area of data governance which specifies how data needs to be handled, what can and cannot be shared and what needs

For BIS use only, New Delhi:2021-01-08 16:08:56

to be absolutely protected keeping privacy in mind, who owns the data, etc. There are regulations across the world that govern data security some of which are industry specific.

Some of the data security standards and regulations are:

a) Health Insurance Portability and Accountability Act (HIPAA)
b) Payment Card Industry (PCI DSS) standards
c) Sarbanes-Oxley Act (SOX)
d) GDPR (European Union)
e) COBIT
f) Personal Data Protection Bill of Govt. of India

8.14.2.2 There are different methods and technologies to secure data in transit and for data at rest. Some examples are given below:

a) Data at rest:
   1) Encrypted file systems,
   2) Storage encryption, or
   3) Database level encryption.
b) Data in transit:
   1) SSL/TLS for end-to-end encryption; and
   2) Network link level encryption.

8.14.3 *API Security*

Applications are built module by module adding new functionalities and capabilities by building on top of or making use of existing functionalities and capabilities. Common functionalities are built in such a way that it can be used by multiple other functional modules through well-defined interfaces called Application Programming Interfaces (API). Typically, these are internal within the application or some of them are exposed for developing surround applications. With the advent of Smart devices and IoT devices computing power is embedded in everyday objects and they communicate using APIs.

As field devices expose their functionalities and capabilities as APIs for integration with higher layer domain applications, security of who accesses those APIs and what they access becomes important. Today all field IoT smart devices have API capability and provide device control and data transmission over well-defined API interfaces. This ensures that even if the device is upgraded to a new hardware or a new firmware, as long as the API is maintained, the higher layer domain solutions can continue to access the data or provide device level management.

If such APIs are not properly secured, unintended access can provide a wealth of information to a Cyber attacker and often give full control over the device, thus a Smart city cannot rely on the authenticity of the data that it transmits.

API security is the protection of the integrity of APIs — both the ones that are owned by the Smart city and the ones that are consumed by Smart city solutions. Broken, exposed, or hacked. APIs are behind major data breaches. They expose sensitive medical, financial, and personal data for public consumption. That said, not all data is the same nor should be protected in the same way. How API security is approached will depend on what kind of data is being transferred.

Many of the application security standards such as OWASP are applicable for API security as well.

8.14.4 *Security Emergency Management*

Prevention is better than cure. While a smart city may take all preventive measures to protect its physical, logical and information assets, it should still be prepared to handle (cure) any emergencies arising out of a cyber-attack or major security impact-intentional or unintentional-to its ICT infrastructure and information assets. Threats and attacks can come from anywhere, both from inside and outside the organisation and it is best to be prepared for it than to be taken by surprise.

It is the responsibility of the cyber security team, in consultation with the executive management team, to implement the following strategies, some of which are preventive measures:

a) A team of professionals to enable communication, collaboration and cooperation in emergency management strategies, looking at the "big pictures" on identifying critical information;
b) Mitigate the organization's threats and vulnerabilities;
c) Conduct organizational and environmental risks against benefits analysis;
d) Monitor and screen employees' responsibilities to prevent insider threats;
e) Update the organization's policy, regulations and employee agreements, along with the organization system, threats and vulnerabilities;
f) Protect the organization's information;
g) Continue systems' updates;
h) Back up full system requirements off-site; and
j) Continuous user education on Cyber security.

8.14.4.1 Emergency management function is more procedural in nature, process driven and involves a substantial number of manual interventions and decision-making processes, while the ICT solutions and tools deployed play the role of the front-end warriors preventing any further emergencies.

This function typically involves the following activities:

a) Assessing the damage and the extent of information loss;
b) Identifying residual risks, vulnerabilities;

For BIS use only, New Delhi:2021-01-08 16:08:56

c) Procedures for cleanup and restoration of services to a state prior to that of the attack;

d) Procedures to prevent further attacks; and

e) Appropriate communication to the internal and external users, the stakeholders, the press and the citizens.

8.14.5 *IP protection and Data Loss Prevention*

With the huge amount of data and compute processing power at its disposal, right from the field level, a smart city can create its own unique set of solutions for better citizen services and create statistical or analytical models to solve certain urban/city specific issues, in collaboration with local industries, academia and research institutions[2]. Such solutions are the intellectual property of the smart city and so need to be protected from infringement and unauthorised use. According to the world intellectual property organization intellectual property is creations of the mind; inventions, literary and artistic works, symbols, names, images, and designs used in commerce. For many organisations, intellectual property may be more valuable than its physical assets. As a result, establishing policies and mechanisms to guard against intellectual property loss or theft is critical. Leakage of such monetizable data and intellectual properties of a smart city should be prevented by formulating a strategy and measures to understand the sensitive models and data they hold, how it is controlled, and how to prevent it from being leaked.

Data loss can be divided into leakage and disappearance or damage which are sometimes overlapping and key drivers for establishing data loss prevention mechanisms include regulatory compliance and intellectual property protection. An effective data loss prevention program should consist of the following essential components:

a) *Manage* — Management functionalities should also include data loss reporting capability and incident remediation workflow management.

b) *Discover* — Discovering and inventorying unique solutions, models, sensitive data at rest in file servers, databases, document and records management, email repositories, and web content and applications; and scanning for sensitive data stored on the endpoint including laptops, desktops, and workstations at remote offices in order to inventory, secure, or relocate that data.

c) *Monitor* — Monitor the use of sensitive data and models, understand sensitive data usage patterns and gain 360-degree visibility of their usage.

d) *Protect* — Enforce security policies to proactively secure data and prevent sensitive data from leaving the organisation. Make sure a clear data classification and governance is in place.

When properly integrated, these four essential components offer effective protection of enterprise valuable information assets. Best practices for data loss prevention is a serious challenge for organizations, as the number of incidents continues to increase. Identifying and blocking all sensitive data is neither possible as an outcome nor wise as a goal. However, with a more focused goal of preventing the most damaging leaks and establishing better ways for users to exchange information securely, data loss prevention can be effective, practical, and successful.

8.15 Geo-Spatial Enablement

A city administrator needs a map to understand the city, it's assets and properties. In other words, Maps are communication language between city administrators and city. Geographical Information Systems (GIS) as depicted in figure 14 provide a layered information about every aspect of the geographical space of a city with locational, planning, development and construction, engineering, operation and maintenance and management related data and information.

GIS converts the data with spatial dimension into thematic information, which offers a knowledge about the spatial entity through different spatial analytical and modelling techniques offered by GIS platform, which helps in better understanding of relation between spatial entities and finally enables decision support system through Spatially enabled 2D and 3D dashboards.

[2] "Data loss prevention," https://tsapps.nist.gov/publications

For BIS use only, New Delhi:2021-01-08 16:08:56

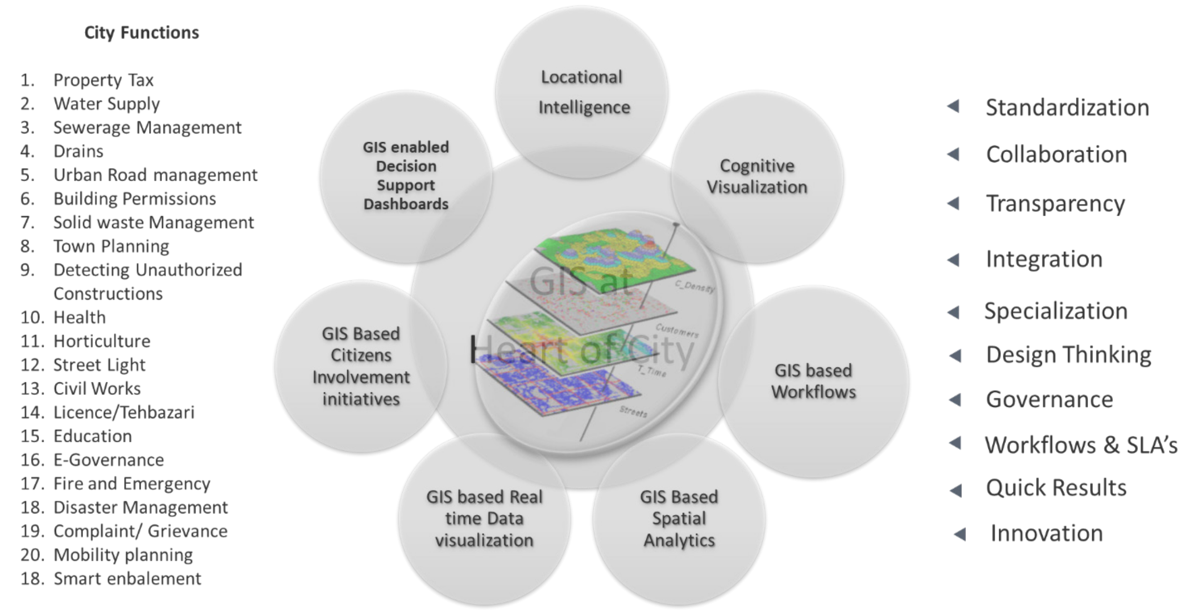


FIG. 14 GEO-SPATIAL ENABLEMENT VIA GIS PLATFORM

GIS is the foundation technology of any city as it provides the language of communication with the city. GIS provides a set of systems for the city as listed below:

a) System of record:

1) The GIS enables government agencies and departments to manage the authoritative and locational records of assets and resources across a city; and

2) Many city departments may be already using GIS to do this: like, planning, land records, electricity and property tax and so on.

b) System of engagement:

1) GIS provides the framework to share knowledge and understanding, through location-aware maps and apps that are available across different devices (including mobile devices), anywhere, anytime; and

2) Organisations shall be able to easily engage with stakeholders, businesses and individuals; seek feedback on plans and initiatives; and share open data and apps on important topics.

c) System of analytical insights:

1) GIS shall enable detailed analysis and understanding to be sought and patterns to be identified, leading to insights on city systems and characteristics including congestion, crime, spending patterns and people movement.

d) System of spatial design thinking:

1) GIS enables spatial design thinking by emphasizing the spatial aspects of city problems and needs ideating solutions incorporating different spatial alternatives and finally testing its impact on the area.

8.15.1 Location information can be found in administrative departments and agencies across all cities. However, connecting this and the relevant departments via a common location platform, that enables the implementation of the systems listed above, is a step that many cities with a smart agenda now need to take. Once the location platform is in place, it enables a whole range of activities and benefits, including:

a) Better decision making:

1) Where best to target capital spending, ensuring that money spent has the best return on investment; and

2) Enabling GeoDesign, where the impacts on existing natural and built systems are considering during the planning process for new infrastructure.

b) City efficiencies:

1) Improved asset utilisation and management, and ensuring maintenance is performed where needed to maximize the useful life of assets; and

2) Like optimising transport services by studying passenger demand and usage patterns, route optimisation of public vehicles and transit services and responsive junction signals that ensure traffic keeps flowing and keeps congestion to a minimum.

For BIS use only, New Delhi:2021-01-08 16:08:56

c) Operations:
   1) Control centres that provide a common operating picture of the entire city, with all systems visualised holistically and in context with one another; and
   2) Scheduling of field activities and monitoring of field crews and assets.
d) Communication:
   1) Engagement with the public on city initiatives and plans;
   2) Transparency into city operations and spending; and
   3) Sharing of city data with the wider community including developers, start-ups, NGOs and academia.

Spatial information is pervasive and primary. When organized using the concepts of space and time, information about cities can be the basis for many powerful services, analytics and decision-making. As the GIS is a system of records, engagement and insight, it is the enabler of the objectives of smart cities.

9 TECHNOLOGY REFERENCE MODELS

9.1 Smart City's Unified Digital Infrastructure

There are four key components listed below that constitute a smart city's digital infrastructure as shown in Fig. 15.

a) ICT infrastructure consists of compute, storage and communication networks that form the bedrock over which the digital infrastructure is built.
b) IoT systems bring in data from various sources (people, processes, applications, physical world) and provide a major part of the fuel to build a smart infrastructure.
c) Platforms, tools and services provide essential tools and services that can be shared across a host of applications, as well as help in management of the entire digital infrastructure.
d) Application services and components make up the smart city applications which deliver the requisite value to all the important stakeholders.

The components are explained in **9.2** to **9.5**.

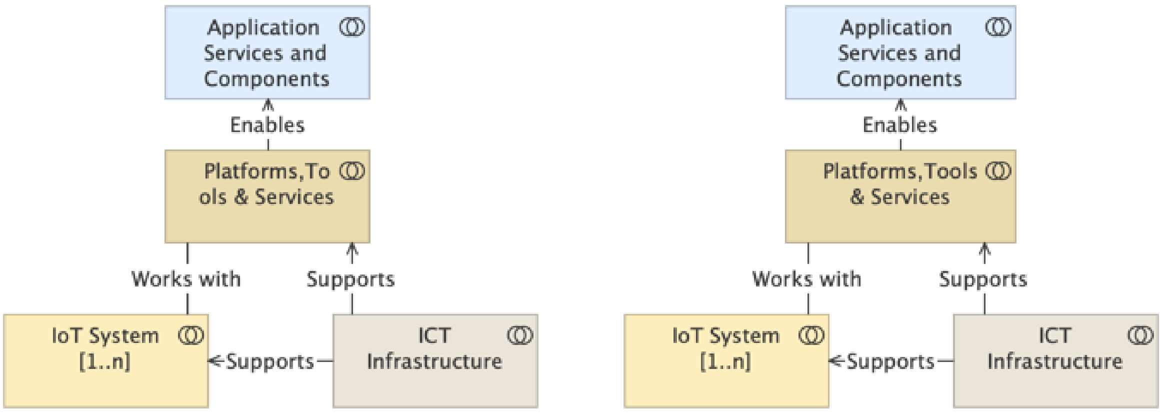


FIG. 15 TECHNOLOGY REFERENCE MODEL FOR SMART CITY'S DIGITAL INFRASTRUCTURE

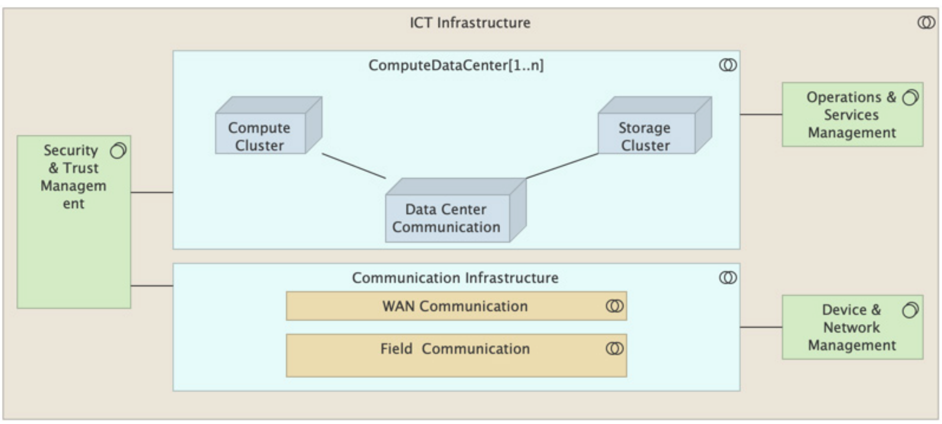


FIG. 16 ICT INFRASTRUCTURE TECHNOLOGY REFERENCE MODEL

For BIS use only, New Delhi:2021-01-08 16:08:56

9.2 ICT Infrastructure

The backbone for any smart city will be the compute-data centres that provi de the substrate on which all the digital tools, services and storage will run and the communication networks that interconnect all the devices deployed as part of the UDI. There could be one or more such centres. These could be located on-premises or in the cloud. Multiple such centres could also be configured to provide redundancy to handle disaster management and recovery. ICT infrastructure technology reference model is depicted in Fig. 16.

Three important functional requirements that are necessary to securely and effectively operationalize and manage this infrastructure are:

a) *Operations and Services Management* — This is a collective of software tools and processes that allow the management of all the resources inside and across the compute data centres, and enable the effective utilization of the centres.
b) *Device and Network Management* — This is a collective of software tools and processes that allow the management of all communication and field device related resources.
c) *Security and Trust Management* — This is a collective of software tools and processes that allow realization, configuration and enforcement of various security and trust related policies.

9.2.1 *Compute-data Centre*

The basic ingredients of this substrate are listed below:

a) Compute cluster consists of compute nodes made of general-purpose processors (CPUs) and may have specialized processors (like GPUs and other customized processing units). These run all the software tools and applications for the UDI.
b) Storage cluster consists of nodes made of memories, hard disks, non-volatile memories as well as archival memories like tape etc., and are available as data clusters. These provide the physical medium to store all the data associated with UDI.
c) Data center communications consists of all necessary equipment to interconnect the nodes of the compute and storage clusters securely and efficiently. These will typically consist of routers, switches, firewalls etc.

The compute-data centres could be small and locally hosted on-premises of a city administration's office. Alternatively, they could also be obtained as a service from a cloud provider (as Infrastructure as a service).

A city might also have combinations of both-called a hybrid cloud, as well as have the services obtained from multiple cloud providers (multi-cloud).

The city might also have devices in the field, which could offer capabilities of local compute and storage, in which case, fog-edge cloud also becomes a part of this hybrid/multi-cloud framework.

9.2.2 *Communication Infrastructure*

9.2.2.1 *Field communication*

A multitude of field devices provides the city's digital infrastructure the capability to interact with the physical world. The communication network that ties them together with the city's digital infrastructure has many possibilities and can be wired or wireless. Some of the common technologies are listed below.

a) Wireless technologies:
   1) GSM/LTE as 3G/4G/5G which is the backbone of cellular service;
   2) WiFi, WiFi6, 6LoWPan, BLE etc.; and
   3) Sub-GHz like IEEE 802.15.4, NB-IoT, LoRA, etc.
b) Wired technologies:
   1) Ethernet (over copper and optical fibre),
   2) GPON (over optical fibre), and
   3) Field device networks like Modbus, CANBus, ProfiBus etc.

These networks will usually have a set of base stations/access points/gateways, that connect the field network to the internet (wide area network).

9.2.2.2 *Wide area network (WAN) communication*

Interconnection over the scale of a city or a district is achieved using WAN and usually is built on fibre optic technologies. The network layer will be based on IP (Internet Protocol) with other layers overlaid on top (like MPLS). Various advanced networking functions like SDN (Software Defined Networking), VPN (Virtual Private Networking), Network Slicing etc. could be used for large cities with advanced digital infrastructures to use more efficiently, provision, adapt to real-time needs and manage the network resources.

9.3 IoT System

A reference model for an IoT system is shown in Fig. 17.

For BIS use only, New Delhi:2021-01-08 16:08:56

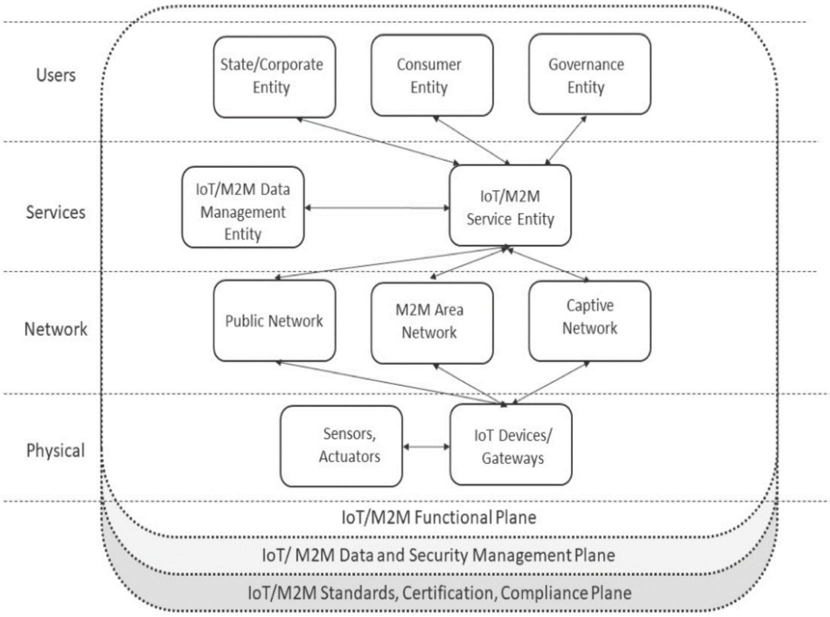


FIG. 17 IOT SYSTEM TECHNOLOGY REFERENCE MODEL

IoT field devices range from sensors (pollution, cameras, pressure, wind, rain, water flow, microphones, touch screens etc.) to actuators (valves, pumps, switches, streetlights, displays, speakers etc.). These will come in a variety of forms (smartphones, feature phones, IoT devices, etc.).

The field devices are connected to the external networks through IoT gateways. The IoT gateways are usually the end points of a larger IP network that interconnects all the elements of the city's digital infrastructure.

IoT servers host the data being generated by the field devices. This data could be further processed or stored in raw form. The data (or its derivatives) will be made available to the city's digital infrastructure from the IoT servers through standard protocols.

The IoT servers might also expose additional services-especially when the field devices are capable of actuation. The services are also exposed through the IoT data and service sharing interfaces.

IoT application software is specific to an application domain and helps to marshal the IoT data, transform it as well as extract additional insights and information from the data coming from the field devices. This software could have components that are distributed across the IoT system stack.

IoT system management software is generally domain agnostic and is used for management of the various components (software, hardware, security etc.) of the IoT system.

Many standards are available for IoT device management, like OMA-DM, OMA-LWM2M, TR-069, etc.

Many standards for communications are available like HTTP, AMQP, MQTT, COAP etc.

9.4 Platforms, Tools and Services

Platforms, Tools and services layer (*see* Fig. 18) is the glue that ties the ICT infrastructure and the IoT systems with the Application services and components by providing the required frameworks for data stores, message queues, application integration, data governance, data transformation, etc. On the one hand, these components ingress, aggregate and transform the various forms of data coming from different sources, both cyber-physical and application. On the other hand, they constitute the relevant tools and services to present meaningful information and interfaces to the Application Services for the stakeholders to view the information and enable them to make the right decisions at the right time.

9.4.1 *Application and Services Integration Platforms, Tools and Services*

Typical stakeholders and users of application and services integration platform tools (*see* Fig. 19) and components are the developer community, application development startups, application architects, owners and administrators and they use different discrete but interacting and interrelated set of components.

App developers and the dvelopment community are more concerned with the developer ports, tools, API documentation, etc., for creating new applications based on the services provided by these components. Typically, these are external to the organisation though there can be a thriving internal developer community that uses these components and services.

For BIS use only, New Delhi:2021-01-08 16:08:56

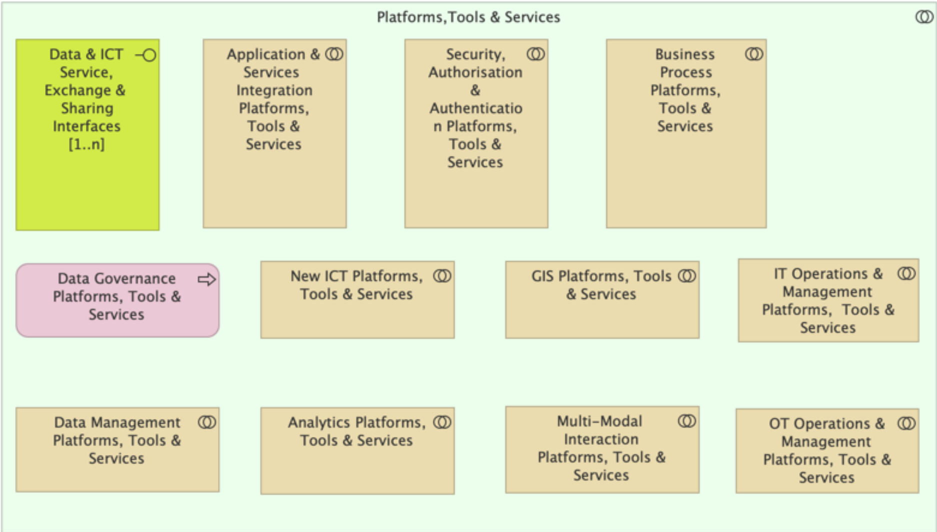


FIG. 18 PLATFORMS, TOOLS AND SERVICES TECHNOLOGY REFERENCE MODEL

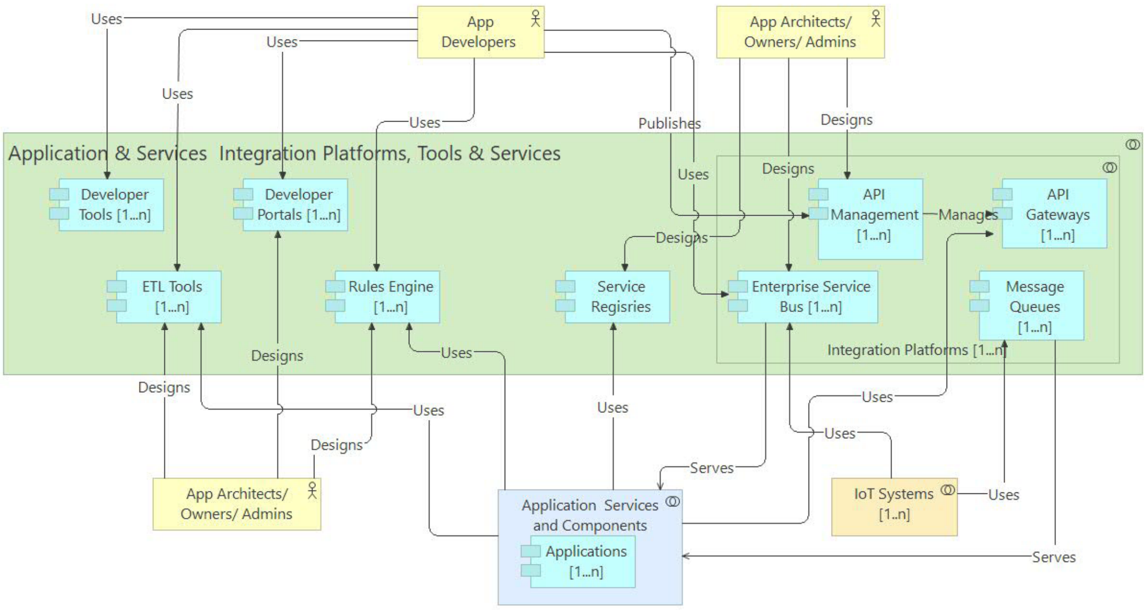


FIG. 19 APPLICATION AND SERVICES INTEGRATION PLATFORM

App architects, owners and admins are generally internal to the organisation and are concerned with architecting, designing and managing these components that help the developer community in creating new applications for the Smart city. Thus, the App architects, owners and admins play an enabling role.

An enterprise service bus (ESB) implements a communication system between mutually interacting software applications in a service-oriented architecture (SOA) or microservices. It represents a software architecture for distributed computing promoting agility and flexibility between applications. Its primary use is in enterprise application integration (EAI) of heterogeneous and complex service landscapes. The ESB is implemented in software that operates between the applications and enables communication among them. Ideally, the ESB should be able to replace all direct application to application interactions so that all communication takes place via the ESB. The beauty of the ESB lies in its platform-agnostic nature and the ability to integrate with anything at any condition. Though no global standards exist for ESB concepts or implementations, the components that form part of the ESB are standards based such as message-oriented middleware.

For BIS use only, New Delhi:2021-01-08 16:08:56

Extract, transform, and load (ETL) is the process by which large amounts of data are extracted from disparate data sources and consolidated into a single database. In the extraction phase, data is parsed and evaluated for suitability. During transformation, data is manipulated to achieve the format required for storage. Some common transformations include the elimination of unnecessary columns, calculation of computed values, and translation of values such as dates into a common format so that the data can be consolidated. The data is then loaded into the database at a frequency and scope consistent with the organization's needs.

Some of the standards that govern the components are:

a) *Platform Standards* — W3C standards define an open web platform for application development that has the potential to enable developers to build rich interactive experiences, powered by vast data stores, that are available on any device. Although the boundaries of the platform continue to evolve, industry leaders speak nearly in unison about how HTML5 will be the cornerstone for this platform.

b) *Message Queue Standards* — Advanced message queuing protocol (AMQP) is an approved OASIS and ISO standard that defines the protocol and formats used between participating application components, so implementations are interoperable.

c) *The MQ Telemetry Transport (MQTT)* — is an ISO standard (ISO/IEC PRF 20922) supported by the OASIS organization. It provides a lightweight publish/subscribe reliable messaging transport protocol on top of TCP/IP suitable for communication in M2M/IoT contexts.

d) *Open API Specification* (OAS) defines a standard, language-agnostic interface for RESTful APIs that are human as well as machine readable. This standard cover API Management and API gateway components. (source: https://www.w3.org/standards).

9.4.2 *Data Management Platforms, Tools and Services*

Technology architecture should be effectively designed (for example, ingestion, data storage, cleansing) to handle the variety, volumes and velocity of big data, allowing it to be easily understood and retrieved by different users. Data management platforms, tools and services is shown in Fig. 20:

a) Data layer should persist data in real time and batch;

b) Should support data models, data marts and cross functional, self-service BI and dashboards; and

c) Should support persistence of semi and unstructured data and structured data sets beyond 1 year for advanced analytics.

Smart cities shall utilize tools such as Petabyte scale data warehouse, in-memory business warehouse and Hadoop based big data infrastructure to manage and store large data sets. Further, cities shall use ETL (extract, transform, load) tools for data integration and transformation. These tools help cities bring together data from multiple systems into a single place and transform it for better insights.

9.4.3 *Data Governance Process, Tools and Services*

A smart city shall utilize data governance tools to implement the functionality described in **8.12** and depicted in Fig. 21. These tools shall be enterprise grade to ensure availability across departments and functions in a smart city.

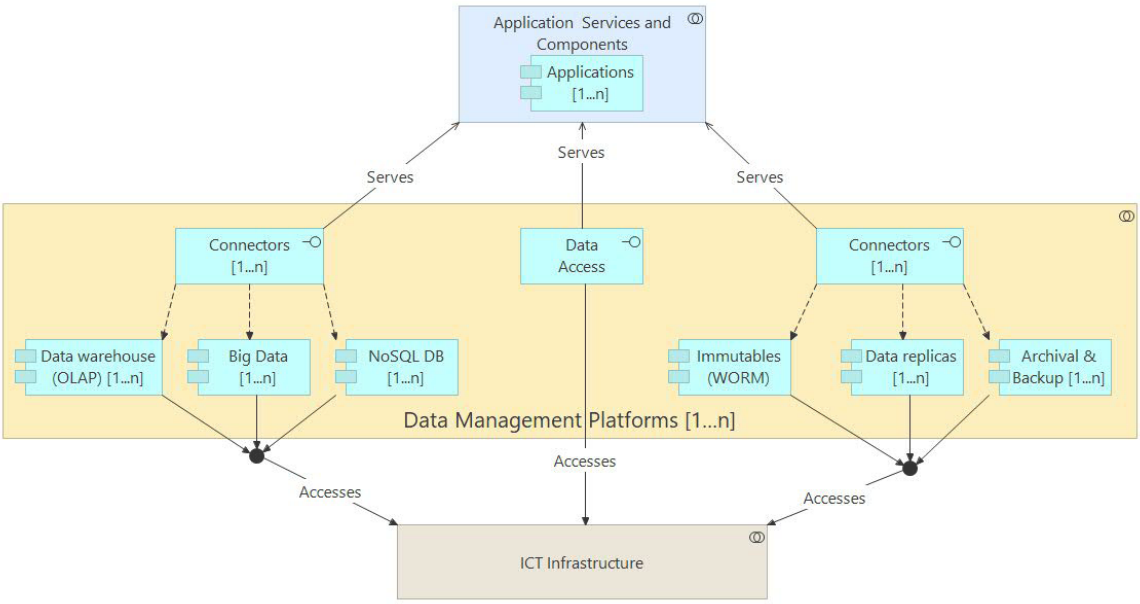


FIG. 20 DATA MANAGEMENT PLATFORMS

For BIS use only, New Delhi:2021-01-08 16:08:56

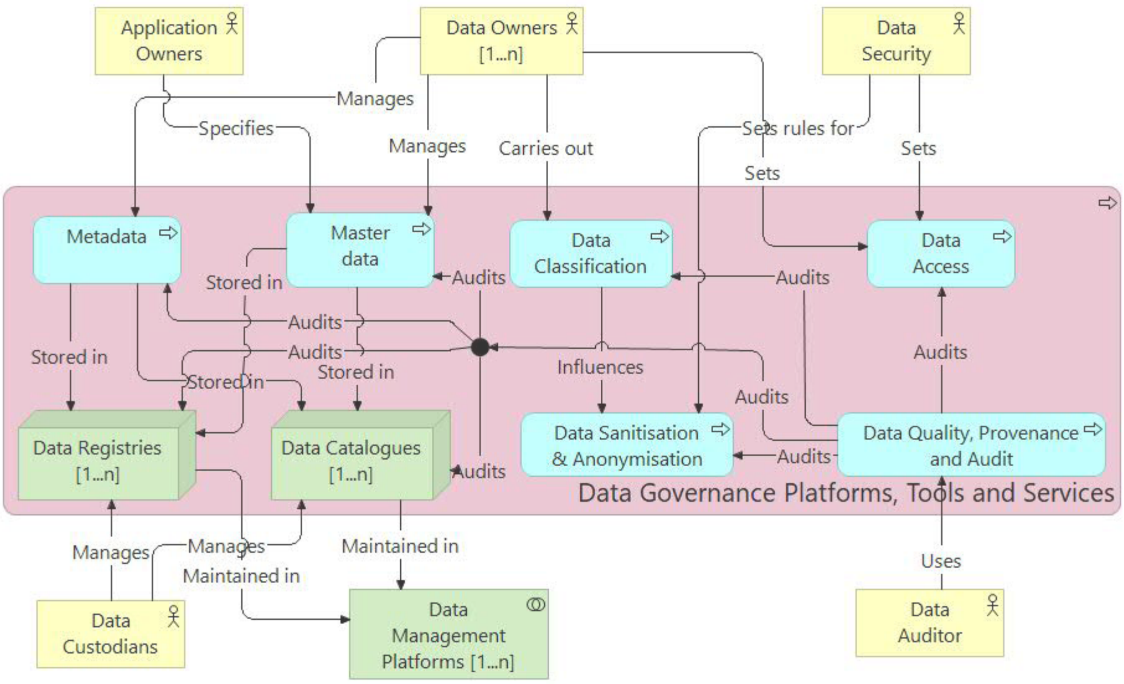


FIG. 21 DATA GOVERNANCE PROCESS, TOOLS AND SERVICES

9.4.4 *Analytics Platforms, Tools and Services*

Extracting meaning and insights from data and then using them to drive the various business processes will be the true hallmark of a smart city.

9.4.4.1 *Tools and platforms*

Various tools and platforms exist to provide classical analytics capabilities and are built on top of structured data (which might be stored in relational databases). These tools could be standalone or be integrated with database engines.

These are usually easy to use and targeted as business users so that they can easily extract operational insights.

They support enterprise business intelligence, self service capabilities. Many tools have a low cost footprint and are open source.

They also provide connectivity to data in cold and warm storage, allowing for both real time dashboarding for most current data and analysis of data beyond 1 year seamlessly.

The platforms should be able to handle big data and allow for exploratory data analysis, workflow automation and component registry management features to support data discovery and mining.

9.4.4.2 *Machine learning and artificial intelligence (ML and AI) frameworks*

Handling unstructured data and creating deeper models from them require using techniques from Machine learning and artificial intelligence.

ML and AI frameworks usually work on unstructured data like text, speech, video as well as structured data.

These frameworks allow:

a) Development of new tools and services based on custom needs and new kinds of data; and
b) Model building, model deployment, and model validation.

9.4.4.3 *Privacy preserving analytics*

Advent of new techniques has now made it possible to perform analytics on data, without sharing the raw data to untrusted users.

These frameworks include distributed or federated machine learning, edge analytics, confidential computing etc.

9.4.5 *GIS Platforms, Tools and Services*

Geo-spatial enablement for smart cities can be provided by GIS platforms, tools and services.

Interconnected GIS platforms from multiple departments/organizations will allow a complete geo-spatial map of the city to be constructed, with different platforms providing different layers.

Besides providing basic services of serving geo-spatial data, GIS platforms can also provide value added services, like answering complex geo-spatial queries.

Platform capabilities of geospatial hub is summarized in Table 5.

For BIS use only, New Delhi:2021-01-08 16:08:56

Table 5 Platform Capabilities of Geospatial Hub

(*Clause* 9.4.5)

	Enterprise GIS Properties
a)	COTS based configurable open standard platform
b)	It shall have Base map provisions with templatized urban management solutions to be easily used by Non-GIS experts. It may also include CAD tool set and 3D mapping.
c)	Ensure data storage and management around a GIS database
d)	Domain specific data model
e)	Should follow an open architecture
f)	Shall have open APIs
g)	Must be OGC certified for seamless integration. It shall support open geo-spatial consortium (OGC) and open web services, such as WMS, WFS, WCS, WMTS, WPS, KML, GeoJSON and I3S for 3D rendering
h)	Shall have integrated image processing capabilities
j)	It shall be device independent and OS independent
k)	Shall incorporate the GIS ready format (2D and 3D) for drone images
m)	Shall be multiple RDBMS supported
n)	Shall provide seamless integration to IoT sensors
q)	Shall facilitate versioned editing
r)	Shall facilitate COTs based advanced locational analytics
s)	Shall facilitate advanced Geo-Processing, Geo-coding, Geo-fencing, Geo-tagging, Geo-triggering
t)	COTs based integrated content management, user management with single sign-on and enterprise log-in (Active Directory LDAP)
v)	Shall support system security architecture at application level, network level, OS level and RDBMS level.
q)	Support standard applications development tools in order to enable app developer ecosystem
r)	The system shall be big data ready with ability to ingest unstructured data and unlabelled data
s)	The system shall be cloud ready
t)	Promote enterprise data sharing at internal and external levels
u)	Facilitates workflow based configurable dynamic spatial dashboards
v)	Workflow based integrated web and mobile apps
	Use ML and AI to train and inference using tools designed to solve urban spatial problems
w)	A hub framework to combine data, visualization, analytics, and collaboration technology to enable governments and citizens to work together on real-world initiatives that tackle the most pressing issues in their communities.

When implemented on the enterprise level, GIS leverages an organization's existing resources in data, staff, and funds by eliminating redundancies and streamlining processes. It also provides qualitative improvements in operations by responding to issues of accountability and customer service.

9.4.5.1 *Enterprise gis platform conceptual architecture*

Enterprise GIS platform connects maps, apps, data, and people in ways that help organizations make more informed and faster decisions. It accomplishes this by making it easy for everyone in an organization to discover, use, make, and share maps from any device, anywhere, anytime. Furthermore, it is designed to be flexible, offering these capabilities through multiple implementation patterns and approaches. Together, these capabilities and flexible approaches make it easier for you to extend the reach of GIS across the enterprise.

The Apps section illustrates the components of the platform that most users interact with, including end-user applications such as field apps, dashboard apps, descriptive information storytelling apps etc. Apps connect people and their business workflows to the platform. Apps are typically used in workflows that follow one or more of the patterns of use (mapping and visualization, data management, field mobility, monitoring, analytics, design and planning, decision support, constituent engagement, and sharing and collaboration). For example, the sharing and collaboration pattern extends geospatial capabilities to everyone in the organization by providing a destination (website and simple apps) where knowledge workers, executives, and field workers can discover, use, make, and share maps. A person capturing data in the field with mobile apps is following the field mobility pattern. A decision-maker using operations Dashboard to observe the real-time information created by field workers is following the decision support pattern. The Portal component of the platform organizes users and connects them with the appropriate content and capabilities based on their role and privileges within the platform. The portal uses a person's identity to deliver the right content to the right person at the right time. The portal provides access controls, content management capabilities, and a sharing model that enables users to share information products across the organization.

The infrastructure component includes the hardware, software, services, and data repositories that are the core of the enterprise GISs System. Numerous best practices, including load balancing, high availability, workload separation, and publication strategies, are linked from and associated with the platform infrastructure. The external systems and Services components include other systems that either provide services to Enterprise GIS or consume GIS services to geospatially enable their capabilities. The ability to easily geo-enable other enterprise business systems is a key capability of enterprise GIS.

9.4.6 *Multimodal Interactions Platforms, Tools and Services*

Stakeholder interactions can span multiple modalities like text, voice and video.

For BIS use only, New Delhi:2021-01-08 16:08:56

They can also span multiple languages.

The interaction medium can be via messaging to smartphones, SMS, emails, phone calls, chatbots or other social media platforms or public media platforms like public displays, speakers, radio, TV, news media etc.

Utilizing platforms and building messaging applications over that, will enable more efficient, cost effective and consistent ways to connect various stakeholders.

9.4.7 *IT Operations and Management Platforms, Tools and Services*

Platforms with standardized interfaces as well as many open-source platforms are available to manage various IT services. Use of automation tools will enable efficient handling of repetitive tasks and escalate only important events to human operators for their attention.

9.4.8 *Business Process Platforms, Tools and Services*

Business process design, documentation and implementation tools and platforms using standards like BPMN etc can be used to allow creation and management of various standard operating procedures.

Various platforms provide integration with several well-known IT tools and workflows and have standard interfaces to allow integration into any IT environment. Use of automation tools will enable efficient handling of repetitive tasks and escalate only important events to human operators for their attention.

Standards based documentation of business processes will allow easy sharing of processes across different cities and allow quick adoption of new processes via modification of existing processes.

9.4.9 *Security, Authorisation and Authentication Platforms, Tools and Services*

Diverse platforms based on open standards exist for identity management, single sign on authentication, multi-factor authentication, PKI infrastructure, Authorisation workflows and authorization policy creation and enforcement.

9.4.10 *OT Operations and Management Platforms, Tools and Services*

Platforms based on open standards to manage field devices and other assets. Any globally acceptable standard like OPC can be used as one of the standards for SCADA systems integration.

9.4.11 *Data and ICT Services Exchange and Sharing Interfaces*

Data exchange via standardized interfaces and data models will facilitate interconnection and interoperation of various IT systems.

Catalogues for data and service discovery will allow data and ICT service providers to list their offerings. Standardized representation of this information will allow easy searching and indexing.

Data resources and ICT services exposed via self-described interfaces will allow automating the process of data and service consumption. Existing standards like JSON-LD, SOAP etc can be used for supporting this.

Distributed authorization framework supporting creation of access control policies, and enforcement of policies to regulate access will support a market ecosystem.

9.4.12 *New ICT Services Platforms, Tools and Services*

The UDI needs to be able to continuously evolve with new functionalities and services, which get seamlessly integrated into the existing system.

This can be achieved if standardized application, service and data integration methodologies and tools are adopted.

9.5 Application Services and Components

9.5.1 *Digitalization and Data Capture Tools and Applications*

Tools for scanning, curating and managing documents; Forms for capturing data from people via smartphone apps, web apps, Chatbots, message boards, social media scraping to be used to get citizen/stakeholder feedback; IoT framework to capture data from devices; Application IoT to capture data from applications; tools/applications to digitally enable all business processes, to capture data into a digital form and share via APIs, so they can be used smartly.

This data capture/digitalization needs to be governed by certain key properties like:

a) Privacy preservation of PII;
b) Ownership of data and ability of owner to control its sharing;
c) Non-repudiability via signatures;
d) Data provenance via signatures and other means;
e) Data security via encryption in motion and rest; and
f) Data governance for quality, normalization, access control, retention and archival.

9.5.2 *Multi-Modal Interaction Applications*

Information dissemination via broadcast messaging and one-to-one communication across multiple modalities and technologies will ensure various stakeholders are easily and efficiently connected together.

Smartphone apps, kiosks, web-apps, SMS, chatbots, public displays devices and social media platforms are some of the current methods for interactions. Multi-modal interaction applications is depicted in Fig. 23.

9.5.3 *City Domain Applications*

Applications in verticals like healthcare, mobility, utility, education, retail, labour, trade, etc. allowing for connectivity and solutions to be provided by a broader

For BIS use only, New Delhi:2021-01-08 16:08:56

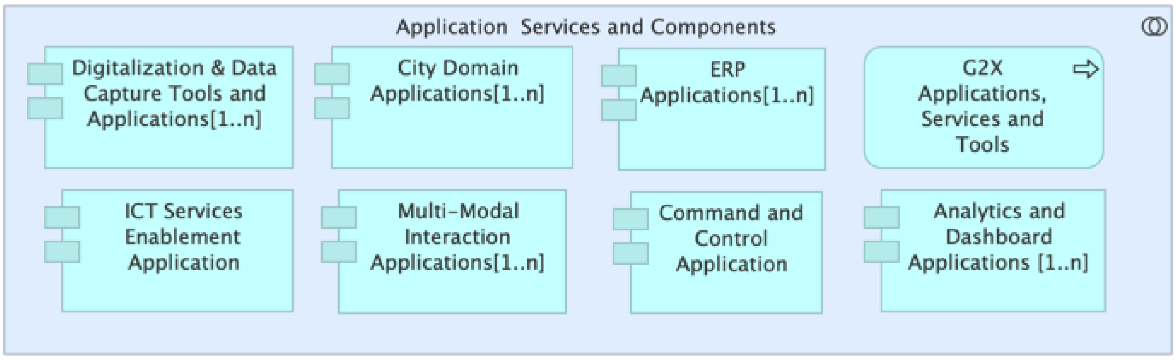


FIG. 22 APPLICATION COMPONENTS AND SERVICES TECHNOLOGY REFERENCE MODEL

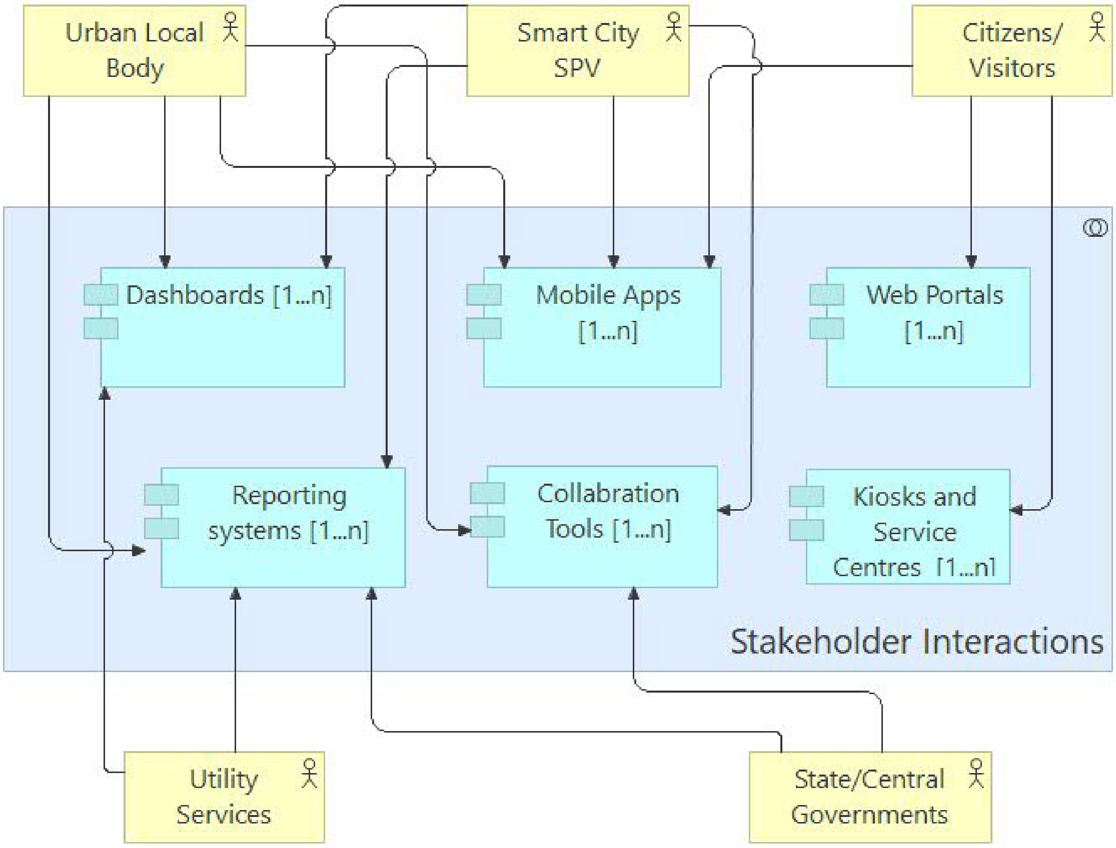


FIG. 23 MULTI-MODAL INTERACTION APPLICATIONS

For BIS use only, New Delhi:2021-01-08 16:08:56

ecosystem, that build on the UDI, will contribute to the richness and effectiveness of the UDI.

9.5.4 *ERP Applications*

A COTS based standardized ERP application to manage, plan and operate all aspects of an enterprise, will allow for efficient implementation of administrative activities. Such applications can also be hosted and offered as services to various departments. The ERP application, while modular, should be capable of providing all the functionality described in section 8.5 out of the box as a single integrated platform. The application should be built to scale to handle an entire city's load and should utilize latest technologies in Enterprise Information management such as in-memory computing and data governance and management.

9.5.5 *G2X Application Services and Tools*

Government to citizen, government to business and government to government services can be automated and digitally enabled via various applications and tools. These will also provide ability to manage the entire business process as well as track the fulfilment of these services.

9.5.6 *ICT Services Enablement Application*

The lifecycle management of ICT applications on the UDI covering their provisioning, resource allocation (in terms of computer, network and storage resources), access control and API provisioning for their interconnection, monitoring for their performance and service levels, will be enabled through this application. In addition, access to the source code repositories (where applicable), will be enabled.

9.5.7 *Command and Control Application*

Integrated command and control centre to oversee the entire operation of a city, will support all the command and control functionalities.

9.5.8 *Analytics and Dashboard Applications*

Insights and dashboards will be generated via these groups of applications.

10 INFORMATION REFERENCE MODEL

The information reference model as depicted in figure 24 consists of the following conceptual models:

a) Data Reference Model: which models data;

b) Data Access Model: which models the access to data;

c) Information Extraction Model: which models the process of information extraction from data; and

d) Insights Extraction Model: which models the process of insights extraction from data.

These models can be extended/instantiated to create concrete models for any use case.

10.1 Data Access Model

Accessing data by any stakeholder involves interacting with a data exchange interface to connect with data sets and then access either the data set as a whole or get specific data items from the set through a selection, or querying process. The data access model is depicted in Fig. 26.

The data set itself gets created by a data collection process, which could be entirely automated or could have human steps.

Each data set has a clearly designated owner (data owner), who is responsible for the data set in terms of providing permissions for sharing/exchanging and sets the policies for the same.

The process of managing the data collection, its curation, normalization/transformation, storage and any other aspects is called data governance and management and is performed by a data steward who is a specialist in these aspects.

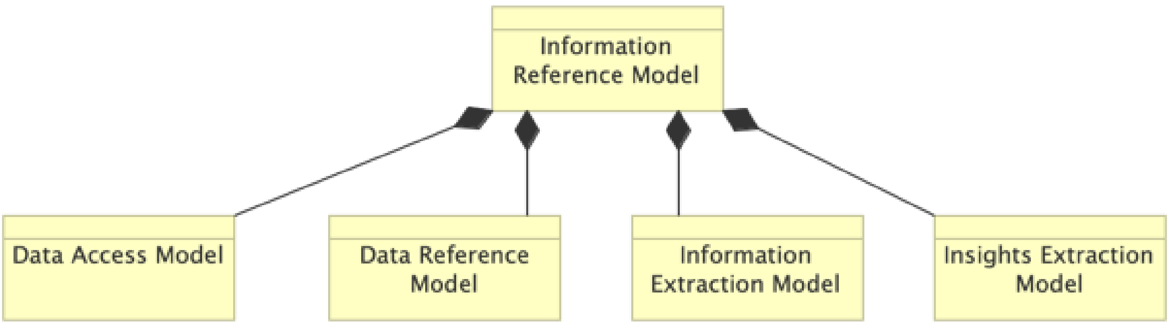


FIG. 24 INFORMATION REFERENCE MODEL

For BIS use only, New Delhi:2021-01-08 16:08:56

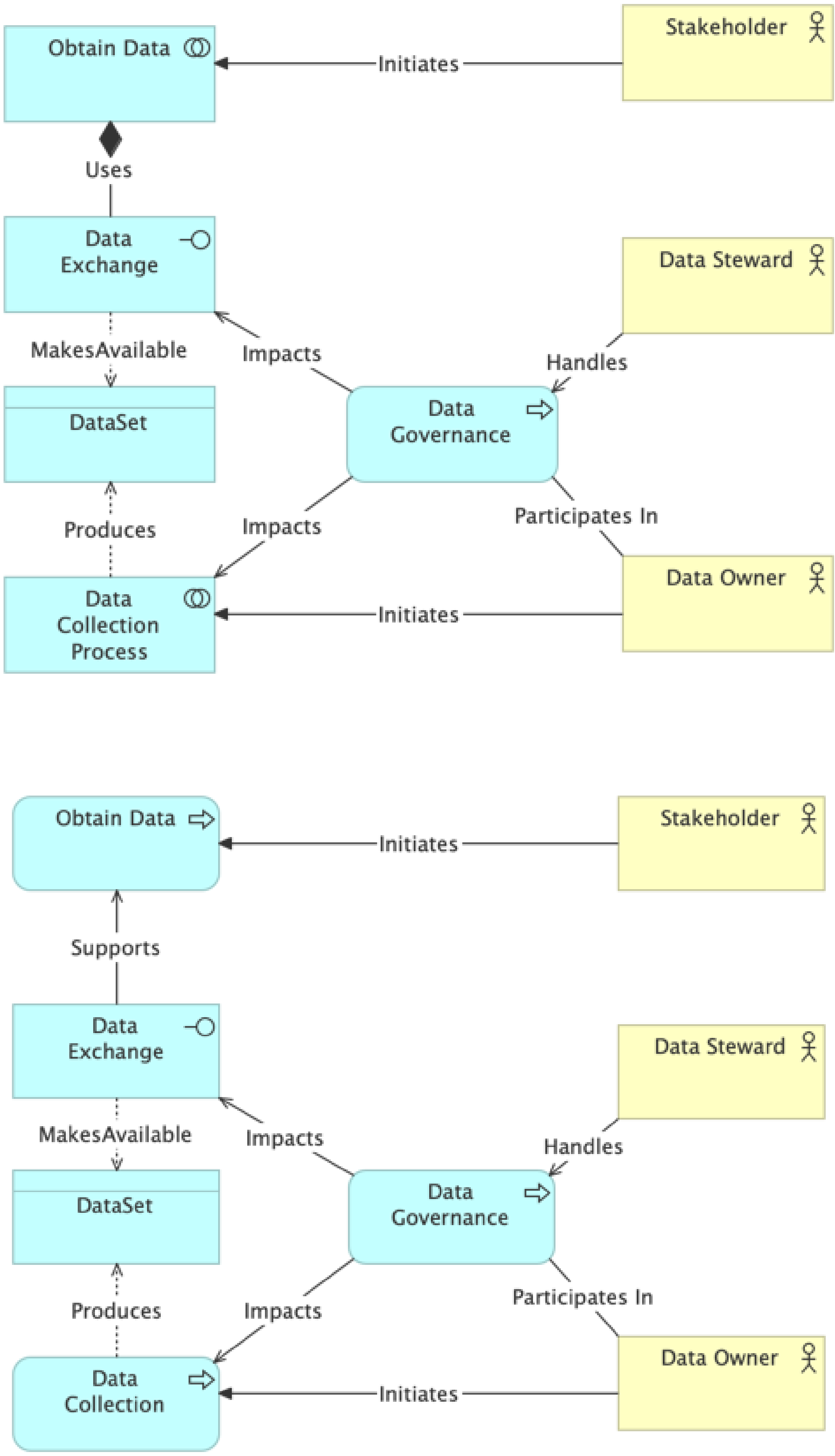


FIG. 25 DATA ACCESS MODEL

For BIS use only, New Delhi:2021-01-08 16:08:56

Example 1: Fault in a circuit breaker triggers an alert for the field agent. Data Owner: Power distribution company. Data Collection Process: IOT enabled continuous monitoring of circuit breaker status. Data Set: Event stream of circuit breaker status. Stakeholder: Maintenance supervisor uses an application, which subscribes to the event stream Analytics of this stream will trigger an alert to the appropriate field agent. Data Steward: Will ensure that this event stream data is made available to the appropriate users. Data Governance: Will ensure that the power distribution company can set the access permissions appropriately for sharing of this event stream.
Example 2: Sharing of current availability of ICU beds in various hospitals Data Owner: Individual hospital. Data Collection Process: Hourly updation via web form or API directly from the hospitals IT system. Data Set: Number of ICU beds and the support capabilities. Stakeholder: Citizens will access this data through their own app (developed by 3rd party). Ambulance service providers and first responders can also use this data during emergencies. Data Steward: SPV will ensure that this data is made available to all health related applications/consumers. Data Governance: Periodic audits to ensure correctness/accuracy/timeliness/liveness/accessibility will be performed as part of this.

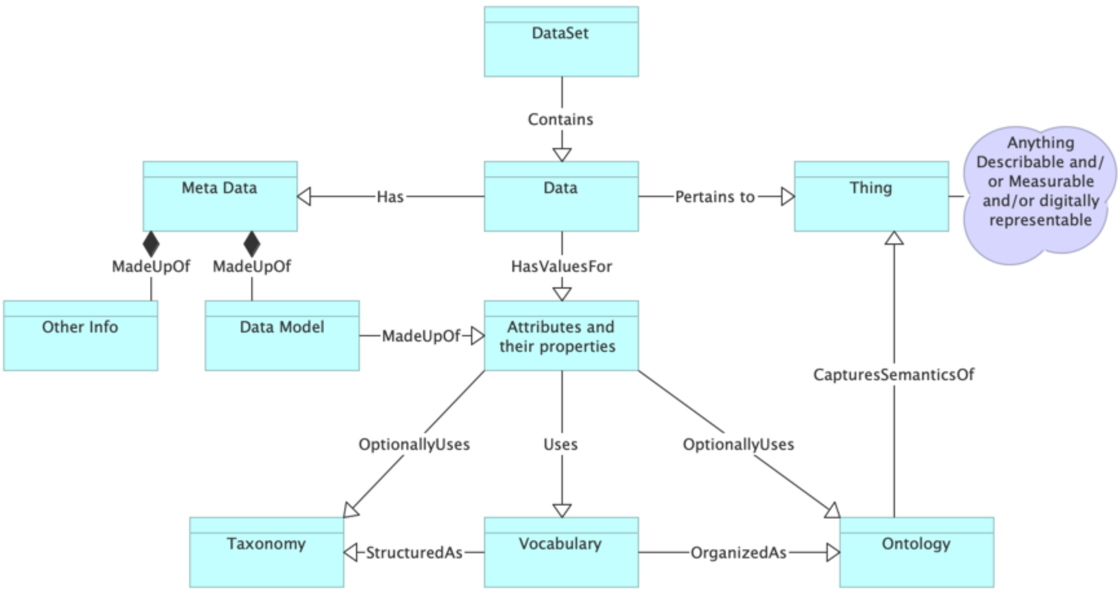


FIG. 26 DATA REFERENCE MODEL

10.2 Data Reference Model

Data is the digital representation about a Thing[3]. Thing is a universal item anything that is measurable, describable or digitally representable, is the subject for data.

Data is contained in a dataset, which is an asset and unit for management and governance[4].

Data can be structured (that is, organized into fields like in a excel file), unstructured (for example, text document) or semi-structured (for example, video streams).

[3] https://schema.org/Thing

[4] InDEA Framework and Federal Enterprise Architecture Data Reference Model v2.0.

For BIS use only, New Delhi:2021-01-08 16:08:56

Typically, structured data has names for the fields (commonly called attributes), and these attributes map to the attributes of the thing. In this document, we represent even unstructured data in this format, wherein the unstructured data has only one attribute (which we can call *data value*, for example, with the content of the *data value* field being the entire unstructured data).

A Data Model as depicted in Fig. 25 describes these attributes and their properties (as far as pertaining to their digital values). A basic data model might stop at listing out the attribute names and the datatypes of the values of the attributes (for example, string, boolean, integer etc.). A data model is an essential ingredient of the meta data (data about the data)[5]. Various standard formats exist for describing meta-data.

A more extensive data model might draw or connect the attribute names to vocabularies which are commonly understood by practitioners in the domain. Further organization of parts of vocabularies as taxonomies (that is, hierarchical or structured arrangement of terms) could provide additional interpretability to the data. A vocabulary might also be organized or structured as an ontology, which captures the meaning (semantics) of the vocabulary in terms of the meaning of the actual Thing, its properties, and its relationships.

The above is an abstract model and specific meta data models, vocabularies, taxonomies and ontologies should be developed for specific domains and standardized, to allow or easy sharing and interpretation of data across different stakeholders.

10.3 Information Extraction Model

Figure 27 depicts Information Extraction Model. *"Information is defined as data that are endowed with meaning and purpose"*[6]. Data needs to be rendered in an appropriate context, in a meaningful way, to make sense to the stakeholder.

A part of the context is provided by the question being asked by the seeker.

For example, to the question "When is bus 276 scheduled to arrive at Mantri Mall stop?" and this provides the context as "The bus 276 will arrive at". In data from the bus schedule, "10.30" is interpreted using the metadata ("description: time, format: UTC"), and is then rendered to provide useful information to the stakeholder.

Data Context is itself data and can also be supplied with data in general. For example, the query "show me where the current accident is" is rendered by showing the accident spot (which is geolocation data), rendered on a map of the locality (which is GIS data).

10.4 Insights Extraction Model

Insights require deeper analysis of data and its context and will usually involve an interactive process of working with data, by a human expert. These also form the basis for creating new analytics as well as predictive models. Once the algorithms for prediction/analytics is finalized, it can be deployed as per the information extration model. Insights extraction model is depicted in Fig. 28.

While the foundation of data, meta-data and data context remains the same, the process of extracting insights is more involved than that for extracting information.

Example: Understanding the spread of an epidemic

To be able to understand how an epidemic spread, one needs to analyse multiple datasets together. These include:

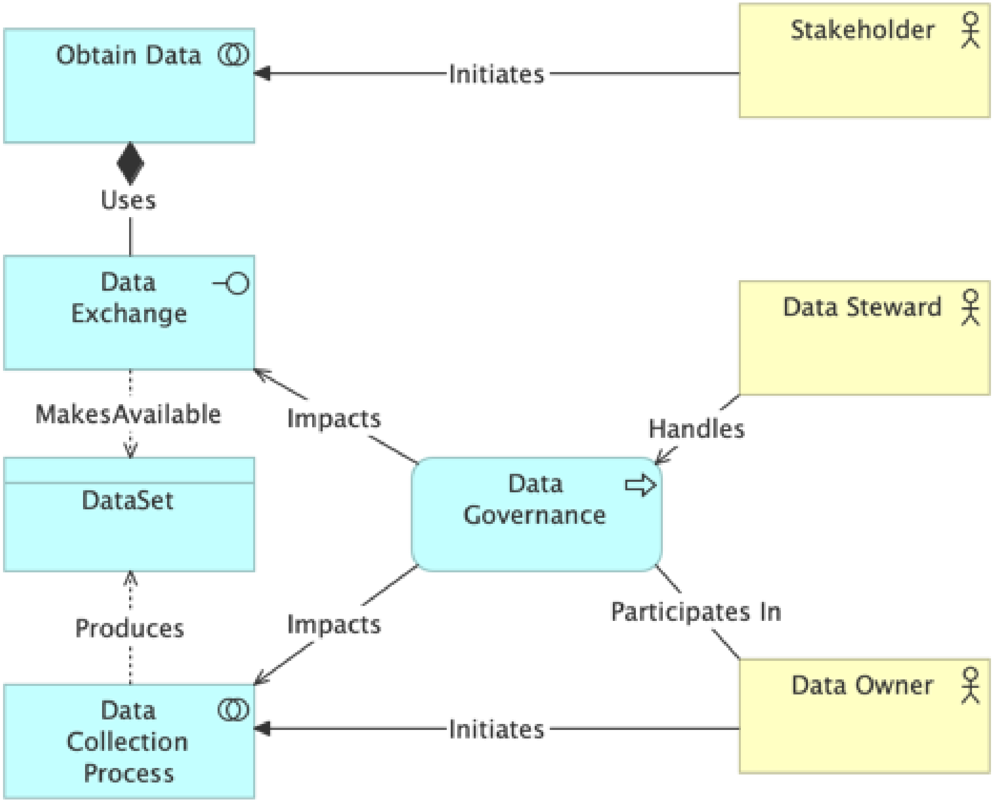
a) symptoms data set as reported by health apps,
b) test reports by testing labs,
c) sales of specific medicines as reported by pharmacies
d) patients admitted with specific symptoms as reported by hospitals; and
e) mobility data as extracted from telecom operators and social media companies.

A joint analysis of all these (and perhaps more) data sets is required to develop an understanding of the spatio-temporal spread of the epidemic. This is an iterative process requiring a continuous back and forth interaction between the human analysts and the data sets, until hypotheses are validated. Once the insights are obtained, these can be converted into predictive models, which can then be deployed to raise alerts about emerging hotspots.

[5] ISO: IEC 11179: Information Technology-MetaData Registries (MDR)

[6] Wallace, Danny P. (2007). Knowledge Management: Historical and Cross-Disciplinary Themes. Libraries Unlimited. pp. 1–14. ISBN 978-1-59158-502-2.

For BIS use only, New Delhi:2021-01-08 16:08:56



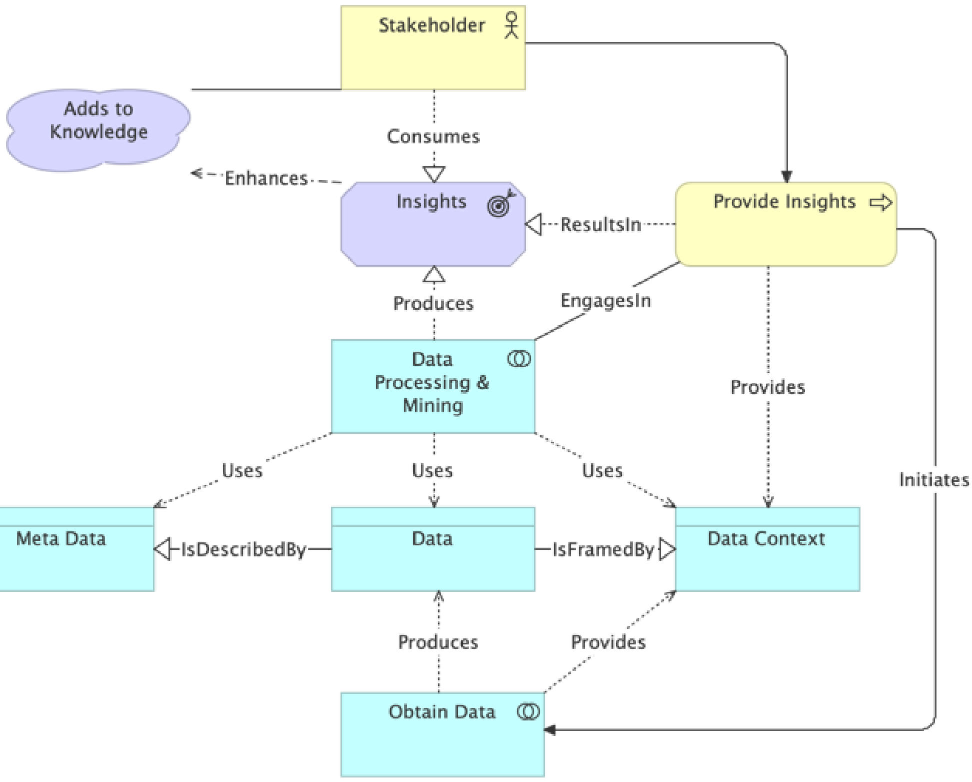


FIG. 27 INFORMATION EXTRACTION MODEL

For BIS use only, New Delhi:2021-01-08 16:08:56

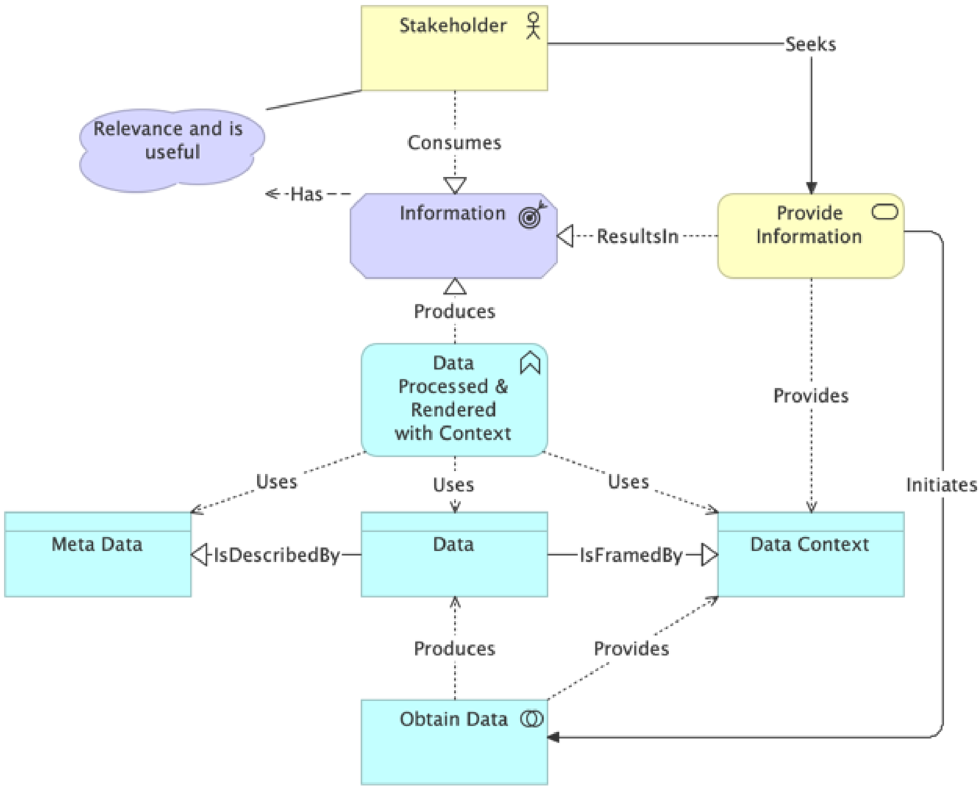


FIG. 28 INSIGHTS EXTRACTION MODEL

For BIS use only, New Delhi:2021-01-08 16:08:56

ANNEX A

(*Clause* 4)

SYSTEM OF SYSTEMS EXAMPLE

A-0 In any city, various departments will be in various stages of creating a digital infrastructure for their own departments. Usually these happen independently and hence leads to Silos. An Integrated Command and Control Centre (ICCC) can be setup to a) bring in relevant data from these various diverse systems into a single place for a holistic analysis and aid in better decision making by the city's municipal corporation, b) better coordinate the actions between various stakeholders namely different public and private service providers, citizens and government bodies, to allow more effective and efficient outcomes of various initiatives and projects.

The abstract architecture described in this standard, is realized as independent service components, but which are interconnected via the ICCC.

A-1 CLASSES OF IT SERVICE COMPONENTS

IT systems can be classified into four main classes, that can be converted into service components via the Data and ICT Sharing functionality of the ICTRA:

a) City Digital Sensing System (CDSS);
b) City E-Government System (CEGS);
c) Citizen Government Collaboration System (CGCS); and
d) City Geographical Information System (CGIS).

A-2 CITY DIGITAL SENSING SYSTEM (CDSS)

Cities are instrumenting their physical infrastructure with sensors and creating a city digital sensing system. CDSS is an IoT platform and the primary entities in this platform are the smart devices (sensing and actuator devices) and smart gateways. Each domain, like transportation, traffic, surveillance, street lighting, environmental monitoring, utility services monitoring etc, can have its own IoT platform, provided by an independent vendor.

The data from these can then be integrated into the ICCC for better decision making, control, management and disaster response. In addition, through the ICCC, the data can be made available to other stakeholders (other departments, citizens etc).

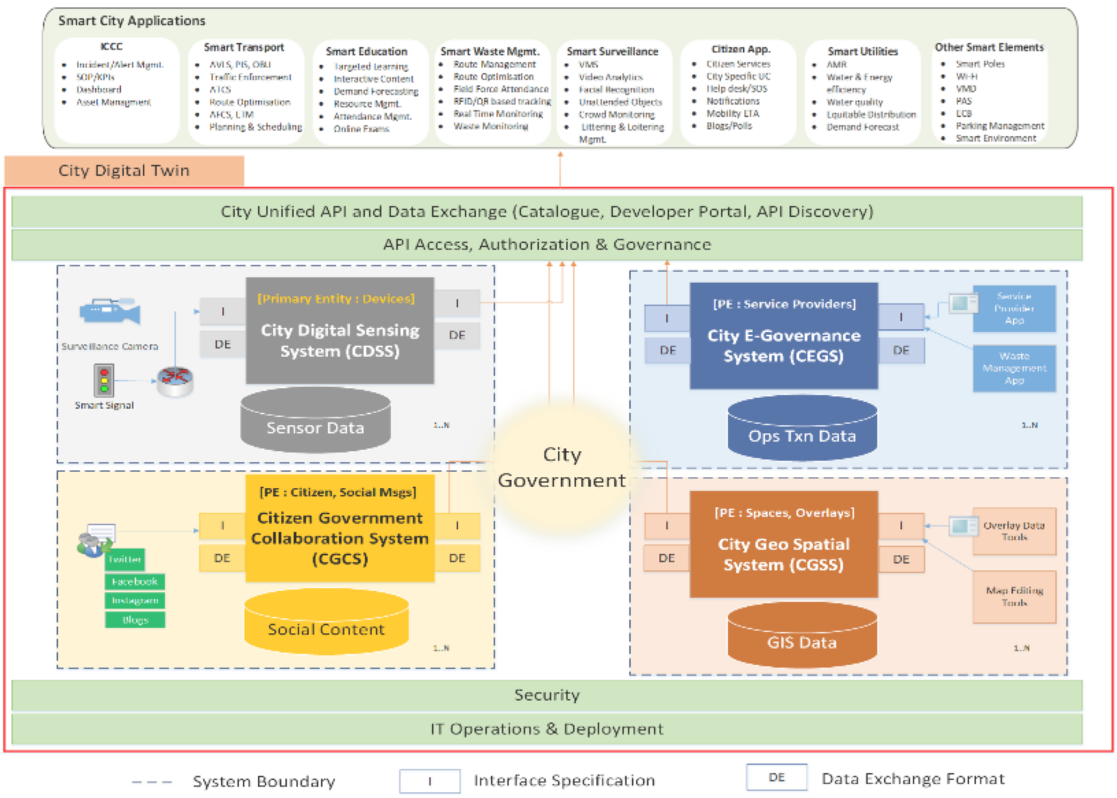


FIG. 29 SYSTEM OF SYSTEMS EXAMPLE

For BIS use only, New Delhi:2021-01-08 16:08:56

ICCC centres are also referred to as digital twins as they represent the digital state of the physical infrastructure. A summary of the key attributes of these systems are:

a) Primary entity: Smart devices and assets;
b) Specification: Device identity and asset identity;
c) Primary data sources: IoT data sensed by the smart devices and non-IoT data sources; and
d) Data Type: Time Series data, video data and device metadata.

A-3 CITY E-GOVERNMENT SYSTEMS (CEGS)

Traditionally cities are managed by municipal bodies through various service provider organizations. Service provider organizations define the workflow and the SLA's to be adhered to in providing a government to citizen service (in general all G2G, G2B and G2C services).

Primary entities in these systems are the service providers and service provider organizations. Through the e-government systems citizens and other stakeholders' requests and services are managed, and tasks are tracked to their closure.

All the service provider IT systems can be integrated with the ICCC via the applications and services connectivity functionality. In addition, the municipal corporation's own IT system for ERP systems can be integrated to allow it to perform its operations more efficiently.

This integration can be facilitated by having each service provider organization provided with a unique identifier. A summary of the key attributes of these systems are:

a) Primary Entity: Service provider organization and service providers;
b) Specification: Service provider identity, service requests
c) Primary Data Source: Service request ID, event ID
d) Data Type: Service request metadata and transactional data

A-4 CITIZEN GOVERNMENT COLLABORATION SYSTEMS (CGCS)

Primary function of the citizen government collaboration system is to manage the interaction between citizens (and other stakeholders like businesses) and the governments. Citizens are the primary entity in this system.

City governments will use these platforms for notifying citizens of key events, developments and achievements in the city. Citizens shall be able to provide their inputs/feedback on the functioning of government in an anonymous way.

This system also has integration hooks with external social networking platforms to pull in information:

a) Primary Entity: Citizen;
b) Specification: Citizen identifier;
c) Primary Data Source: Citizen profile information, social messages; and
d) Data Type: Social messages (textual, images, videos).

A-5 CITY GEOGRAPHICAL INFORMATION SYSTEMS (CGIS)

Most government departments need a GIS system to capture their geographically distributed assets, specific to their domain, in a precise manner. For example, the water utilities board needs to have a precise map of all its piping, water treatment plants, valve locations, field agents, vehicles etc. Another example is the traffic police need precise information of all their stations, surveillance cameras, roads, junctions etc.

The city's ICCC can host a GIS system that provides the base maps including city boundary, municipal boundary, zone boundary, ward boundary, street maps, DEMs, satellite images, land use and all other overlays, like city properties and assets.

All the other GIS systems can provide only additional layers of interest to their domain, while sourcing any other layers as needed from other systems (through the ICCC). This will enable:

a) Better management and update of ground truth (a single entity will be responsible for any layer);
b) Reduce costs via sharing of resources; and
c) Allow better coordination between various entities (road cutting can avoid cutting optical fibre or water pipes).

A summary of the key attributes of these systems are listed below:

1) Primary Entity: GIS Layers;
2) Specification: Asset and layer identifier;
3) Primary Data Source: Base maps, map overlays and other layers; and
4) Data Type: GIS.

A-6 SYSTEM OF SYSTEMS INTERACTIONS – EXAMPLE

This section describes the interaction between various systems for an example use case of Citizen Safety. The interaction diagrams describe the source of the request, the actor performing the request, the primary system of interaction by the actor and the message flow between different systems to complete the use case.

Use Case Scenario: Let us assume that a citizen logs into a social networking platform and tweets that he/she is in danger. The outcome that the city would like to achieve is to identify the location of the citizen in danger, assign tickets to police personnel responsible for (or nearby) to that location to immediately reach out to resolve the issue. Also, the city would like to automatically brighten up the streetlights closer to the area and turn on the cameras to feed in information to the command centre for monitoring and coordination.

For BIS use only, New Delhi:2021-01-08 16:08:56

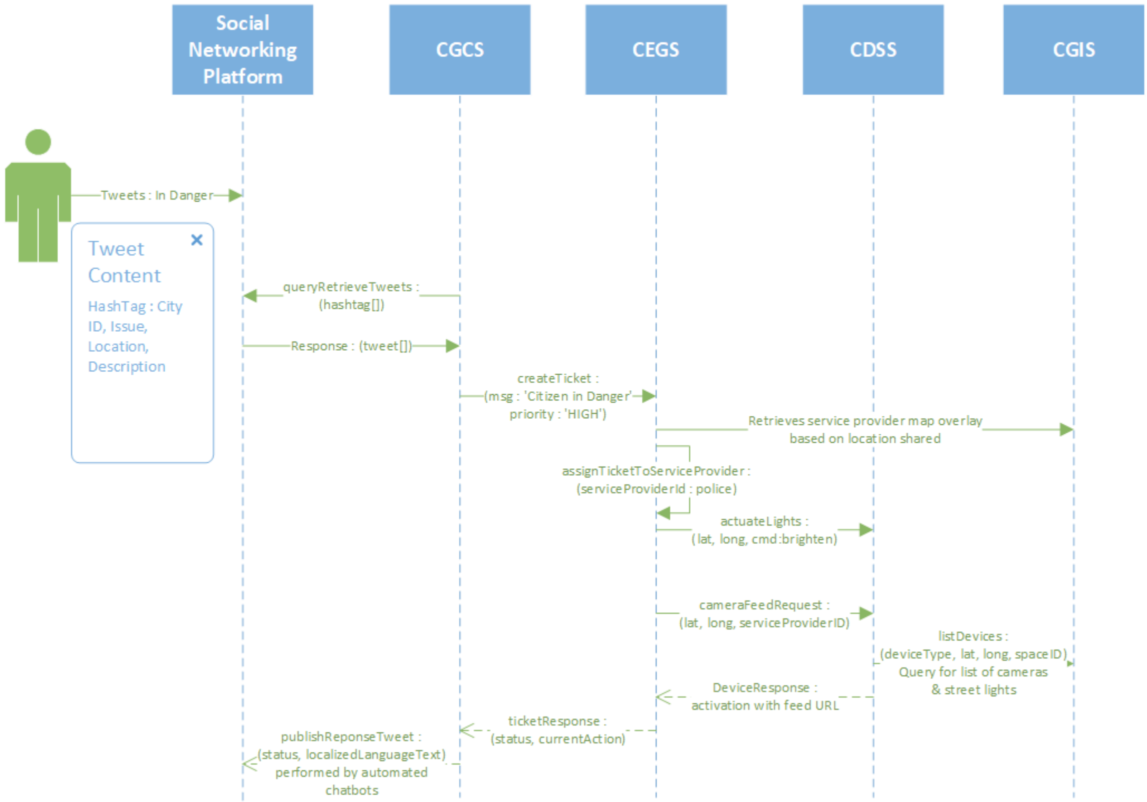


FIG. 30 USE CASE OF CITIZEN SAFETY

Besides this reactive and immediate usage of such a system, further analysis on historical data can be done, leading to better urban planning and deployment of various city resources to make the city safer. This analysis can look at geo-spatial and temporal hotspots of complaints, streetlight lighting levels, citizen grievance reports from the localities, police station locations and FIR reports, public transport locations, etc., can be done in a holistic way, leading to a more comprehensive plan to improve citizen safety levels. However, such analysis will be possible only if data from appropriate government and private systems are brought together.

For BIS use only, New Delhi:2021-01-08 16:08:56

ANNEX B

(*Clause* 4)

REALIZING STAKE HOLDER'S EXPECTATIONS

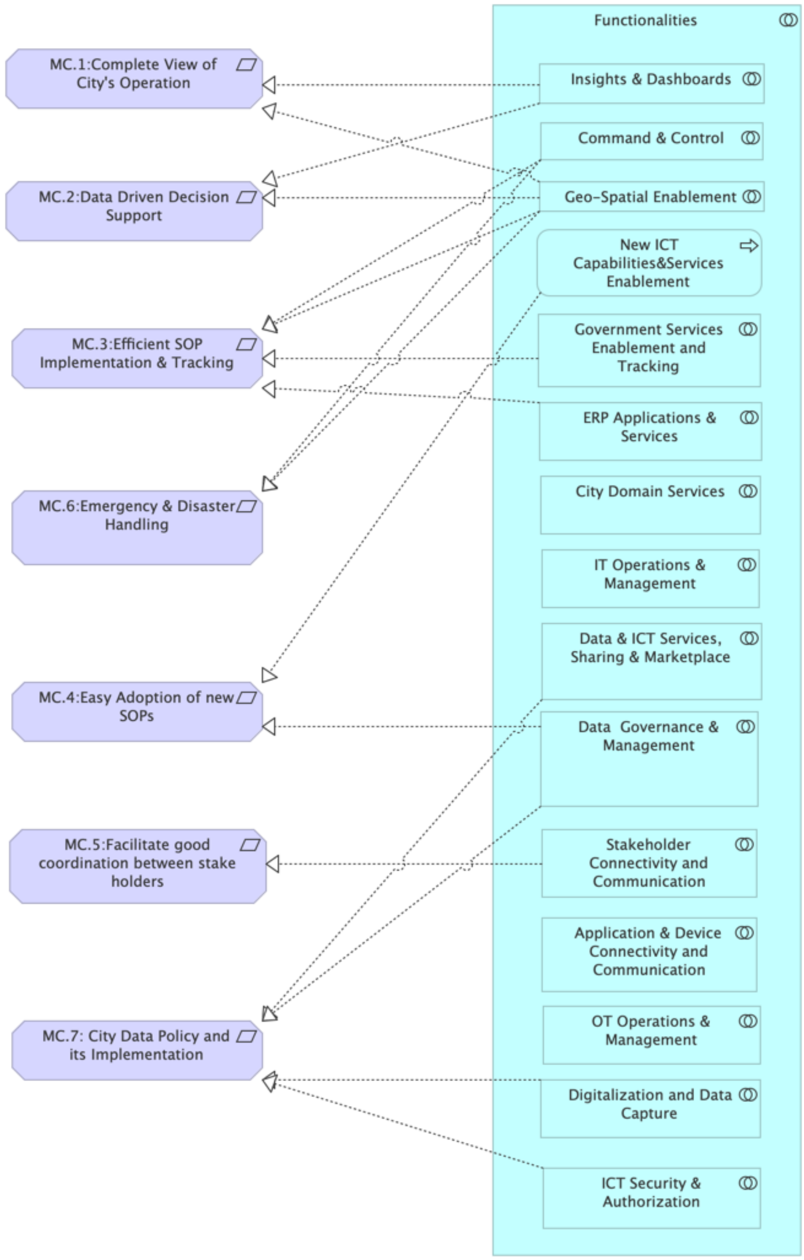


FIG. 31 REALIZING MUNICIPAL CORPORATION'S CONCERNS

Each concern of the municipality is covered by a group of functionalities as described above.

For BIS use only, New Delhi:2021-01-08 16:08:56

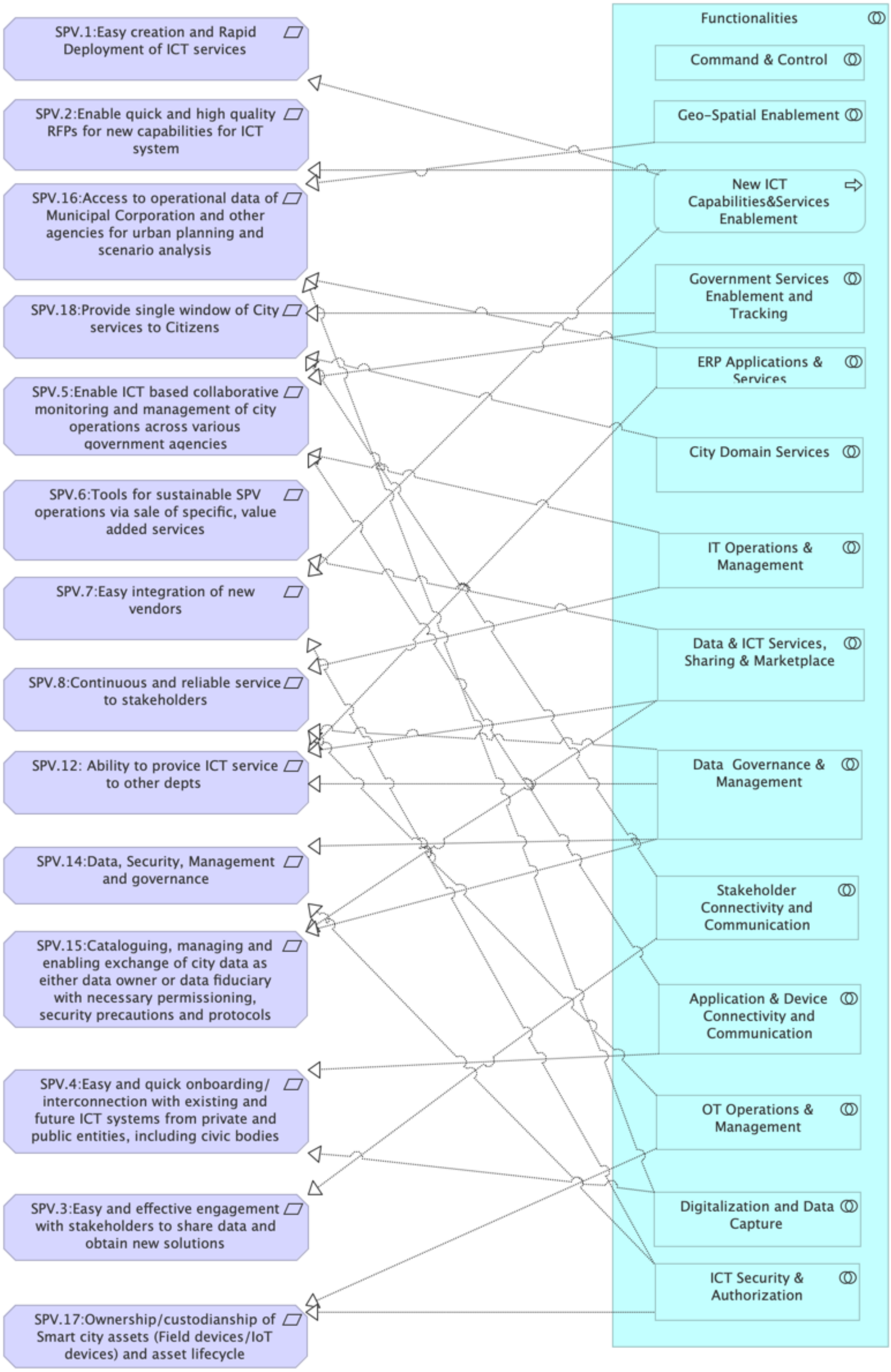


FIG. 32 REALIZING SMART CITY SPV'S CONCERNS

Each concern of the smart city SPV is covered by a group of functionalities as described above.

For BIS use only, New Delhi:2021-01-08 16:08:56

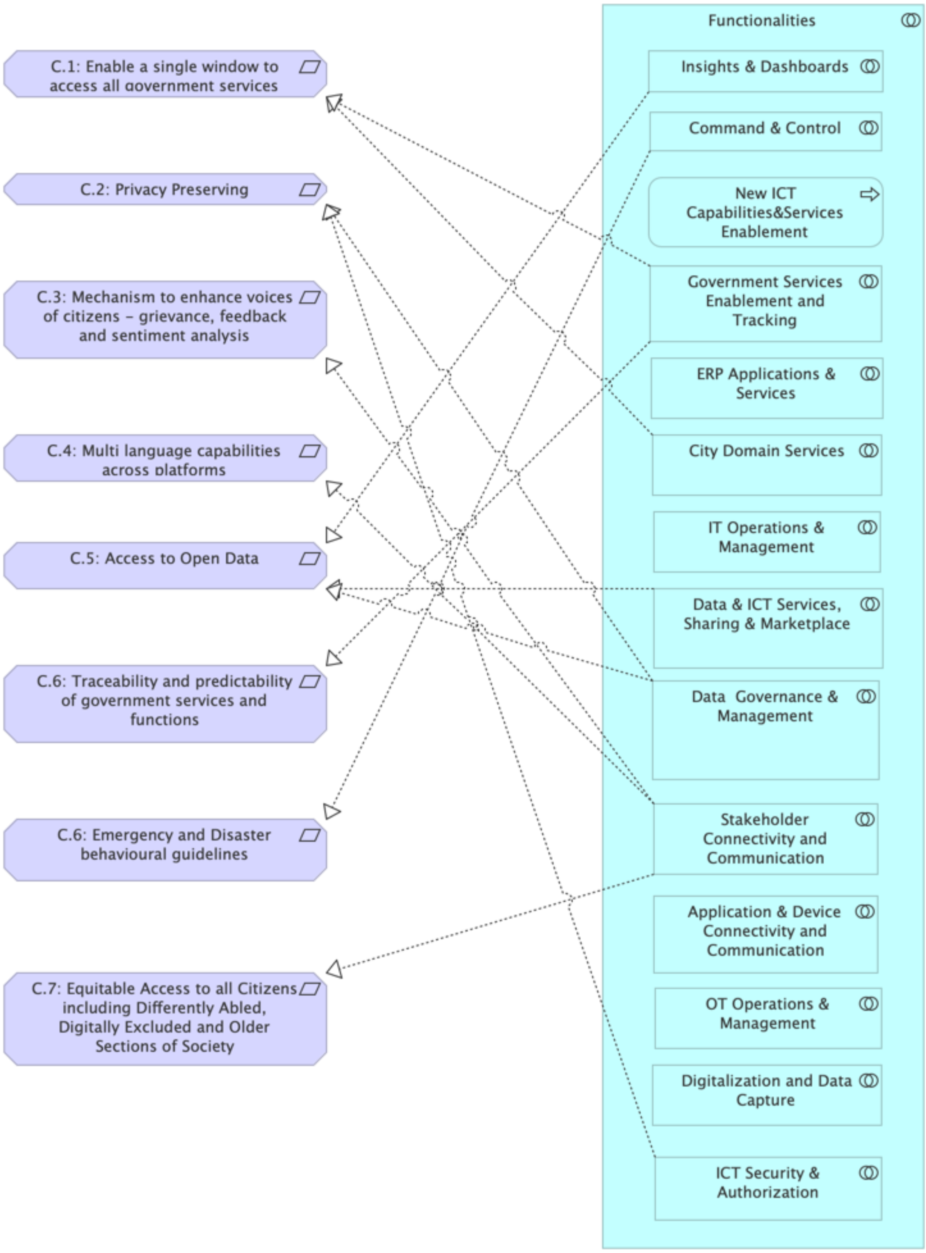


FIG. 33 REALIZING CITIZEN'S CONCERNS

Each concern of the citizen is covered by a group of functionalities as described above.

For BIS use only, New Delhi:2021-01-08 16:08:56

ANNEX C

(*Clause* 4)

REALIZING FUNCTIONALITIES

Each functionality is realized by a combination of underlying components, tools and services. However, to not clutter the diagram, only primary dependencies are denoted.

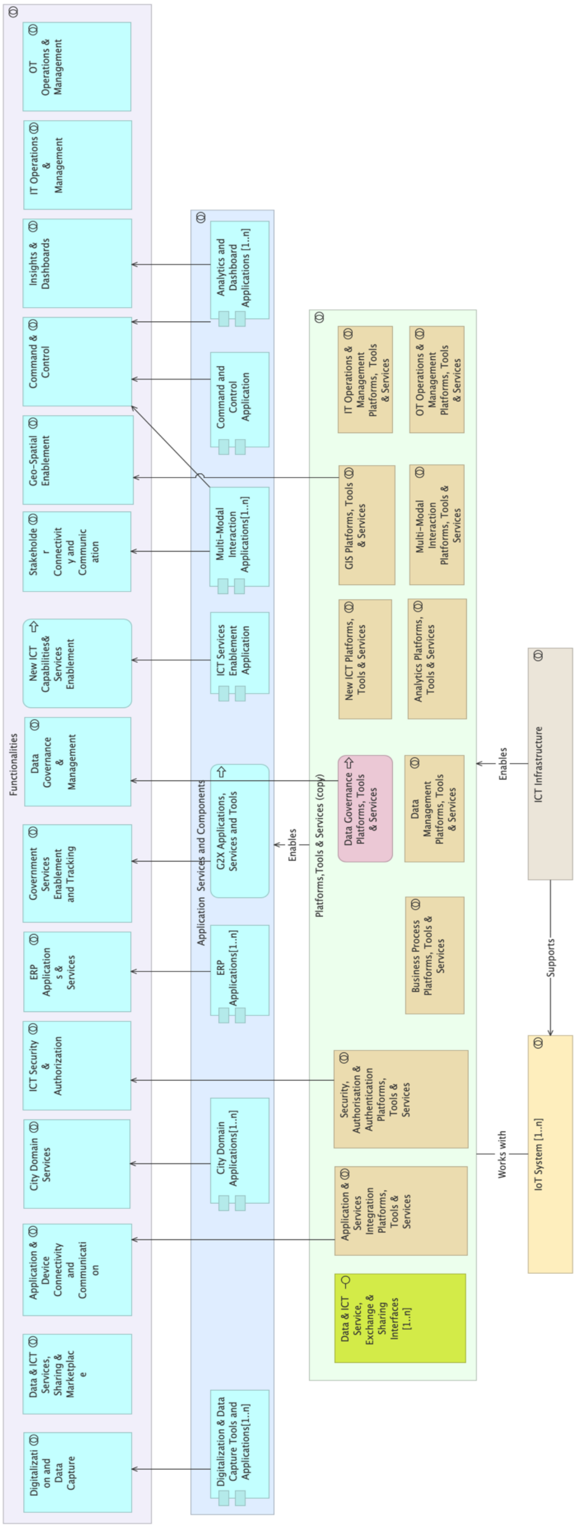


FIG. 34 REALIZING FUNCTIONALITIES

For BIS use only, New Delhi:2021-01-08 16:08:56

ANNEX D

(*Clause* 8.5)

ERP APPLICATIONS AND SERVICES

This section describes in detail the functionalities expected of an ERP system in a city/ULB. The city/ULB shall aim to implement a standard, COTS based solution(s) that works as a single integrated platform for expenditure management and perform day to day administrative functions. The below section describes the functionalities described in section **8.5.1** to **8.5.5** in more detail:

D-1 ACCOUNTS, BUDGET, INVESTMENTS AND PLANNING

D-1.1 Budgeting

Budgeting is a combination of 4 functions, namely:

a) Budget maintenance;
b) Budget execution;
c) Grants management; and
d) Budget closing and financial reporting.

This module helps with maintenance, management, and monitoring of public funds, integrates operational and accounting processes with a maintained budget, help users manage grant information and provide status indicators of the grant process according to the administrative requirements of their sponsors and covers the planning, standardizing, scheduling, and monitoring of financial and budget close activities.

Key features of this module include creation of budget structure, update and approve budgets, allow budget increases from revenue, budget release and reporting. It enables real-time and parallel budget controls that can operate on multiple levels, helping to monitor and control funds while reducing procurement and operating costs. Users can maintain master data components for managing, controlling, and reporting based on the sponsor's administration requirements. Users can further reconcile budgetary accounting data with financial and managerial accounting.

D-1.2 Financial Accounting

An accrual based double entry accounting system covering functionalities like general ledger, accounts receivable and accounts payable. This module is used to record all financial transactions that occur on a day-to-day basis. All postings to accounting are triggered in response to operative transactions. In addition to above, this module covers various accounting flavours such as Asset Accounting, inventory accounting, Joint venture accounting, contract accounting as well as financial closing and reporting.

The system can run an integrated acquire-to-retire cycle for all assets including functions like depreciation, capitalization and post capitalization, value and monitor material and work-in-process inventories according to legal regulations and management accounting requirements and monitor the compliance status, due dates and generate the supported compliance reports. System can also generate and submit ad hoc or non-periodic reports.

D-1.3 Investment and Treasury

Investment and teasury module helps deliver functions like cash and liquidity management, payments and bank communications and debt and investment management. The cash and liquidity function helps monitor cash positions, make bank transfers, approve payments, create cash pools, liquidity planning and perform cash flow analysis and forecasting. The key feature of this module is to forecast the future liquidity trend and track the status and trace liquidity planning cycle to get an early warning indicator of liquidity shortages or to be used as a steering tool for medium-and long-term investment or borrowing.

Further, this module helps streamline, control and gives better transparency into communications with banks. Automated payment workflows streamline routing and approval processes and ensures compliance by using rules-based approval workflows that guarantee proper payment approvals and documentation. Using this module, the system can portray the process for managing liabilities and capital investments, Manage Financial transactions (such as securities, money market, derivatives, securities lending, etc.), manage financial position, calculate NPVs, determine market risks of financial transactions, and so on.

D-1.4 Financial Planning and Analysis

Financial planning and analysis module is a central, integrated place for all financial planning data. It also provides real-time access to master data and actual data to compare with the plan data to determine the success of the financial units. This module captures costs by cost center and defines the output of the cost center in terms of activity types. It allows the city to determine the costs incurred by each product/services in order to successfully manage the portfolio. These costs can be broken down into each step of the value chain mapping the quantity flow with the values of Finance. Finally, it enables the city to analyze the profitability of various cost objects. It shows contribution margins in real time and offers detailed views for further analysis.

For BIS use only, New Delhi:2021-01-08 16:08:56

D-2 ASSET, LAND AND REAL ESTATE MANAGEMENT

D-2.1 Maintenance Operations

Asset management process starts with mapping the operational structures to technical objects to create maintenance master data. This can efficiently manage and evaluate the technical assets and maintenance objects, monitor the costs involved and allow for a faster evaluation of the maintenance data. Maintenance Planning and Scheduling helps the system optimize the scope of work and effort required for inspection, maintenance, and planned repairs. *Maintenance Execution* allows the system to perform planned and unplanned maintenance tasks. It lets users carry out preliminary costing, work scheduling, material provisioning, and resource planning.

D-2.2 Linear Asset Management

Linear Asset Management is another key functionality in the asset management module that enables the management of the entire lifecycle of linear assets like roads, rails, pipelines, or electricity transmission lines. The process helps to optimize the reliability, availability, maintainability, and safety of the networks and infrastructure. It is a comprehensive, integrated process that facilitates and connects linear asset management activities with enterprise processes and data. In addition, the process helps to improve asset management effectiveness, efficiency, and strategy, thereby boosting asset reliability and return on investment.

D-2.3 Resource Management

Resource management provides insights into your maintenance workload and available capacities for current and upcoming maintenance activities. This module allows the system to check current and forecasted work centre utilization, build one or more schedules for a specific target week, and level work centre utilization before dispatching the scheduled work. The user can get an overview of KPIs related to maintenance planning, track utilization of work centres, create one or more schedule simulations for a target week and check the forecasted utilization at weekly and daily level.

D-2.4 Real Estate Management

Real Estate Management is a comprehensive software solution with the ability to boost revenues by managing the real estate portfolio. The module allows the system to create a real estate portfolio and integrate with CAD drawings to create a 3D visualization of the assets. The module allows management of vendor contracts and leases, service charge settlement, property revaluation and any other third party integration. Another important aspect of real estate management is land management. This feature integrates the internal view with the public and legal view of land. The system can depict land registers, parcels and other public registers, link them to other master data objects, set up contracts, and run reports.

D-3 PROJECT (WORKS) MANAGEMENT

D-3.1 Portfolio and Project Management

This module provides a comprehensive and up-to-date view of the entire portfolio of city's projects to present the full extent of project risks and opportunities. It allows the user to overcome delays that can occur, as information is collected from disparate sources. This capability enables the user to define work breakdown structures as a basis for hierarchical project accounting. Users can plan costs and budgets and track actual costs that are tightly integrated with core Business processes including expenditure [financial accounting], maintenance operations, resource management. This provides users with better insight into the project progress and the project financial performance and enables the user to avoid cost overruns in time. The system can monitor purchase requisitions, purchase orders, and account assigned to work breakdown structures as well as monitor planned and actual project progress values.

The system can create and maintain operative networks assigned to work breakdown structures (WBS) and determine the chronological sequence of activities in a network or a standard network. It can schedule activities within a network by determining the earliest and latest start and finish dates for each activity. It helps standardize and improve project execution and reduce associated administrative and system costs, by providing reliable project management functions that can be deployed independently or integrated into the, Human Resources or Financials back-end system.

Portfolio and project management gathers diverse data into dashboards which act as a starting point for portfolio analysis. It lets users carry out financial and capacity planning for capital projects. Users can further evaluate projects based on a set of questionnaires and scoring models to assess the impact of each project as well the risk assessment associated with it. Users can perform What-if analysis by running simulations for budget assignment or capacity assignment.

D-4 PROCUREMENT AND MATERIAL MANAGEMENT

D-4.1 Inventory Management

An inventory management system works on the accepted accounting principle of no posting without a document. According to the document principle, a document must be generated and stored in the system for every transaction/event that causes a change in stock. It supports the recording of actual stock levels

For BIS use only, New Delhi:2021-01-08 16:08:56

(quantities) of materials: Performance of physical inventory (stocktaking) and stock adjustments both for own stock and for special stocks on periodical basis. It also provides stock room management capabilities such as material management on levels like storage bin, unit, batch, stock status, etc., inbound processing, outbound processing and internal warehouse movement.

D-4.2 Procurement Management

Procurement management is an amalgamation of multiple processes such as sourcing, requisitions, purchase order processing, purchase contracts and supplier management. Functions like Self-service requisitioning help to create, manage, and track orders efficiently. The system can create items from external catalogues and free-text items. Purchase order processing issues an instruction to an external supplier to deliver a specific quantity of material at a certain point in time, or to perform services within a specific period. In this module, the system can create purchase orders from existing requisitions, previous purchase orders or from scratch.

Purchase contracts functionality maintains long-term agreements with suppliers regarding the supply of materials or the performance of services within a certain period as per predefined terms and conditions. This module lets the system create, change and display purchase contracts by type value contracts, quantity contracts and so on. Purchasing Analytics provides users with centralized analyses and the necessary capabilities to better understand the procurement areas-both on a holistic level and on a more fine-granular level relating to connected systems. The module enables users to analyse purchase contracts for consumption, analyse overall spend and analyse requisitions all by supplier, item or department.

Finally, the supplier management module gives the system the ability to segment and classify suppliers based on their capability and operational area. The system can create a master data of all suppliers capturing details like tax registration, name, address, bank details etc. Invoice processing functionality lets the system create the supplier invoice with reference to a purchase order or without any reference. The invoice verification checks the supplier invoice for correctness. Before posting the document, the system can simulate the supplier invoice in order to display the account movements.

D-5 HR, PAYROLL AND SELF SERVICE

D-5.1 Core HR and Payroll

This module is where the system maintains the master data for all employees. The system can capture all personnel details like demographic, benefits, compensation, date of joining, and so on. It creates and manages the organization structure, creates, displays or assigns jobs, tasks, or staff assignments, manages funds and budget, and carries out personnel cost planning and analysis. The module provides self service capability to both managers and employees. For the managers, it provides support in planning, analysis, budgeting, recruitment, compensation, employee development, and cost management processes on any device. Employee Self-services gives employees personalized access to their own HR data, processes, and services.

Further, this module enrols employees in benefits plans and terminates enrolments, monitor continuing eligibility for plans, monitor provision of evidence of insurability, administer retirement plans and manage the pension fund including calculation of employee contribution and calculation of total benefits. Payroll function processes and ensures accurate, on-time payrolls for all employees.

D-5.2 Time and Attendance Management

Time and attendance management enables recording and managing time data effectively and efficiently. It provides a comprehensive and effective business concept and related processes for manual and automatic recording of personnel times. It helps define and manage time elements for payroll schedules, and shifts. It further allows to define and manage working calendars and vacation allowances for your organization. Employees can enter absences, attendance, and breaks. Managers can approve attendances and absences.

D-5.3 Skill Management

Skill management helps to maximize employees' utility within an organization. The system can plan and implement specific personnel and training measures to promote the professional development of employees. Two important functions that are a prerequisite to achieving this goal are skill assessment and goals and performance management. These functionalities help to consolidate employee skill profiles for full assessments in a structured and objective approach as well as to motivate the workforce by aligning them with organization goals.

For BIS use only, New Delhi:2021-01-08 16:08:56

ANNEX E

(*Foreword*)

COMMITTEE COMPOSITION

Smart infrastructure Sectional Committee, LITD 28

Organization	*Representative(s)*
Indian Institute of Science, Bengaluru	Prof Bharadwaj Amrutur (***Chairman***)
Amravati Smart City Development Corporation Limited, Mumbai	Shri Siddharth Ganesh
ARM, Noida	Shri Kumaar Guhan
Centre for Development of Telematics, New Delhi	Shri Aurindam Bhattacharya Shrimati Anupama Chopra (*Alternate*)
Criterion Network Labs, Bengaluru	Shri Jayaprakash Kumar Shri Krishna Kumar Lohati (*Alternate*)
Cyan Connode Private Limited, Bengaluru	Shri Deepak Nimare Shri Manish Widhani (*Alternate*)
E-Goverments Foundation, Bengaluru	Shri Krishnakumar Thiagarajan
Ericsson India Private Limited, Gurugram	Shri Sendil Kumar Devar
ESRI, Noida	Shri Vijay Kumar Shrimati Seema Joshi (*Alternate* I) Shri Rupesh Kumar (*Alternate* II)
European Project SESEI	Shri Dinesh Chand Sharma
Hawlett Packard Enterprise,	Shri R. Devarajan
IEEE India, Bengaluru	Shri Srikanth Chandrasekaran Shri Munir Mohammed (*Alternate*)
India Smart Grid Forum, New Delhi	Shri Reji Kumar Pillai Shrimati Parul (*Alternate*)
Indian Institute of Science, Bengaluru	Shri Vasanth Rajaraman
Intel India Technology Private Limited, Bengaluru	Shri C. Subramanian Shri Anantha Narayanan (*Alternate* I) Shri Sidhartha Mohanty (*Alternate* II)
Ministry of Housing and Urban Affairs, New Delhi	Shri Kunal Kumar
MoHUA Smart Cities Handholding team	Shri Padam Vijay
Narnix Technolabs Private Limited, New Delhi	Shri N. Kishor Narang
National Smart Grid Mission, Ministry of Power, Gurugram	Shri Mr Arun Misra Shri Gyan Prakash (*Alternate* I) Shrimati Kumud Wadhwa (*Alternate* II)
PHYTEC Embedded Private Limited, Bengaluru	Shri B. Vallab Rao (Vasu)
Pune Smart City, Pune	Shri Manojit Bose
Qualcomm India Private Limited, Bengaluru	Dr Vinosh Babu James Dr Punit Rathod (*Alternate*)
Renesas Electronics, Bengaluru	Ravindra Chaturvedi Saurabh Goswami (*Alternate*)

For BIS use only, New Delhi:2021-01-08 16:08:56

Organization	*Representative(s)*
Schneider Electric's industrial software business-AVEVA, Mumbai	SHRI GOURAV KUMAR HADA SHRIMATI SANGEETA GARG (*Alternate*)
Secure Meters Limited, Gurugram	SHRI PUNEET KHURANA SHRI KAUSTUBH PATIL (*Alternate* I) SHRI UTTAM KOTDIYA (*Alternate* II) SHRI ANIL MEHTA (*Alternate* III)
Shrama Technologies Private Limited	SHRI AMARJEET KUMAR
Siemens Limited, Mumbai	SHRI PRADEEP KAPOOR SHRI VIKRAM GANDOTRA (*Alternate* I) SHRI MANOJ BELGAONKAR (*Alternate* II) SHRI RAVI MADIPADGA (*Alternate* III)
Standardization Testing and Quality Certification (STQC)	SHRIMATI LIPIKA KAUSHIK
System Level Solutions (India) Private Limited, Anand	SHRI DIPEN PARMAR SHRI FORAM MODI (*Alternate*)
Tata Consultancy Services Limited, Mumbai	SHRI RAMESH BALAJI SHRI DEBASHIS MITRA (*Alternate*)
Tejas Networks Limited, Bengaluru	DR KANWAR JIT SINGH
Telecommunication Engineering Center, Department of Telecommunications, New Delhi	SHRI RAJEEV KUMAR TYAGI SHRI SUSHIL KUMAR (*Alternate* I) SHRI UTTAM CHAND (*Alternate* II)
In Personal Capacity	PROF SUPTENDRANATH SARBADHIKARI
BIS Director General	SHRIMATI REENA GARG, SCIENTIST 'F' AND HEAD (ELECTRONICS AND IT) [REPRESENTING DIRECTOR GENERAL (*Ex-officio*)]

Member Secretary

SHRI MANIKANDAN K.
SCIENTIST 'D' (ELECTRONICS AND IT), BIS

For BIS use only, New Delhi:2021-01-08 16:08:56

Panel involved in the Finalization LITD 28/P6 ICT Reference Architecture

Organization	*Representative(s)*
IISc	Bharadwaj Amrutur (***Convener***)
Intel	Subramanian C.
CDOT	Aurindam Bhattacharya
HP	Devarajan R.
Shrama Technologies Pvt Ltd	Amarjeet Kumar
Egovernments.org	Krishnakumar T.
IISc	Arun Babu
AECOM	P. Vijay Kumar
Arm Embedded Technologies Ltd	Kumaar Guhan
L & T SWC	Omkar Nath
ESRI	Vijay kumar
Secure Meters Ltd	Uttam Kotdiya
Tejas Networks	K. J. Singh
iDeCK	Ramya V. P.
iDeCK	Sushma Nirmal
SID-IISc	Suresh Kumar
SID-IISc	Abhay Sharma
India Smart Grid Forum	Parul Shribatham
Egovernments.org	Gautham Ravichandar
SAP	Tulsidharan V.
Bangalore Smart City Limited	Manjunath D.
SAP	Sujit Patheja
HPE	Manukumar Nair
Pune Smart City	Manojit Bose
Siemens	Ravi Madipadaga
Siemens	Sabi Shaw
ESRI	Ruma Chakrabarty
L & T Infotech	Lavanya Nupur
Tata Communications Limited	Rakesh Trivedi
Tata Communications Limited	Anand Nadar
Tata Communications Limited	Praveen Arora
IISc	Poorna Tejasvi
Secure Meters Ltd	Sajit Panikkar
STQC	Ms Lipika Kaushik

For BIS use only, New Delhi:2021-01-08 16:08:56

BIBLIOGRAPHY

1. https://www.opengroup.org/
2. Maier, Mark W. Architecting Principles for Systems-of-Systems.
3. Lapalme, J., Three Schools of Thought on Enterprise Architecture, IT Professional, vol. 14, no. 6, pp. 37–43, Nov – Dec 2012, doi: 10.1109/MITP.2011.109
4. Service-Oriented Architecture, The Open Group https://www.opengroup.org/soa/source-book/soa/index.htm
5. InDEA Framework (India Enterprise Architecture Framework), Ministry of Electronics and Information Technology, Govt. of India, 2018 (http://egovstandards.gov.in/sites/default/files/IndEA%20Framework%201.0.pdf)
6. Archimate 3.1: https://pubs.opengroup.org/architecture/archimate3-doc/toc.html
7. NIST publication “Data loss prevention”
8. Understanding Command and Control, Alberts, D.S., and Hayes, R. E., 2006, CCRP Publication Series
9. ISO/IEC 11179: Information Technology - Meta Data Meta Data Registries (MDR) (Series)
10. https://schema.org/Thing
11. Wallace, Danny P. (2007). Knowledge Management: Historical and Cross-Disciplinary Themes. Libraries Unlimited. pp. 1–14. ISBN 978-1-59158-502-2.
12. Open Web Application Security Project (https://owasp.org)
13. IES-City Framework https://pages.nist.gov/smartcitiesarchitecture/
14. https://www.w3.org/standards
15. https://www.wikipedia.org/

For BIS use only, New Delhi:2021-01-08 16:08:56

For BIS use only, New Delhi:2021-01-08 16:08:56

For BIS use only, New Delhi:2021-01-08 16:08:56

Bureau of Indian Standards

BIS is a statutory institution established under the *Bureau of Indian Standards Act*, 2016 to promote harmonious development of the activities of standardization, marking and quality certification of goods and attending to connected matters in the country.

Copyright

BIS has the copyright of all its publications. No part of these publications may be reproduced in any form without the prior permission in writing of BIS. This does not preclude the free use, in the course of implementing the standard, of necessary details, such as symbols and sizes, type or grade designations. Enquiries relating to copyright be addressed to the Director (Publications), BIS.

Review of Indian Standards

Amendments are issued to standards as the need arises on the basis of comments. Standards are also reviewed periodically; a standard along with amendments is reaffirmed when such review indicates that no changes are needed; if the review indicates that changes are needed, it is taken up for revision. Users of Indian Standards should ascertain that they are in possession of the latest amendments or edition by referring to the latest issue of 'BIS Catalogue' and 'Standards: Monthly Additions'.

This Indian Standard has been developed from Doc No.: LITD 28 (15990).

Amendments Issued Since Publication

Amend No.	Date of Issue	Text Affected

BUREAU OF INDIAN STANDARDS

Headquarters:

Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi 110002
Telephones: 2323 0131, 2323 3375, 2323 9402 *Website*: www.bis.gov.in

Regional Offices:		*Telephones*
Central	: Manak Bhavan, 9 Bahadur Shah Zafar Marg NEW DELHI 110002	2323 7617 2323 3841
Eastern	: 1/14 C.I.T. Scheme VII M, V.I.P. Road, Kankurgachi KOLKATA 700054	2337 8499, 2337 8561 2337 8626, 2337 9120
Northern	: Plot No. 4-A, Sector 27-B, Madhya Marg CHANDIGARH 160019	265 0206 265 0290
Southern	: C.I.T. Campus, IV Cross Road, CHENNAI 600113	2254 1216, 2254 1442 2254 2519, 2254 2315
Western	: Manakalaya, E9 MIDC, Marol, Andheri (East) MUMBAI 400093	2832 9295, 2832 7858 2832 7891, 2832 7892

Branches : AHMEDABAD. BENGALURU. BHOPAL. BHUBANESHWAR. COIMBATORE. DEHRADUN. DURGAPUR. FARIDABAD. GHAZIABAD. GUWAHATI. HYDERABAD. JAIPUR. JAMMU. JAMSHEDPUR. KOCHI. LUCKNOW. NAGPUR. PARWANOO. PATNA. PUNE. RAIPUR. RAJKOT. VISAKHAPATNAM.

Published by BIS, New Delhi

For BIS use only, New Delhi:2021-01-08 16:08:56