

Internet of Things - Product Lifecycle Management for the Successful Deployment of Smart City Technologies in Saudi Arabia.

Abstract:

The deployment of Internet of Things systems is treated as a technology project, even though the value obtained depends on the situation that exists before installation and on what happens a long time after the system has been put into operation. This review looks at smart-city IoT as a portfolio of product-service assets, with responsibility shared throughout the stages of definition, design, procurement, integration, operation, renewal and retirement. Its objective is to draw together evidence from 2020 to 2025 and to establish a lifecycle management framework for the deployment of smart-city technology in Saudi Arabia. Thirty peer-reviewed sources, all with verified digital object identifiers, were chosen using an integrative review that covered implementation, IoT architectures, cybersecurity, digital twins, edge intelligence, citizen acceptance, sustainability and electronic-waste management. The evidence was analysed in relation to six lifecycle stages and six cross-cutting assurance dimensions. The synthesis reveals that failure in deployment is seldom due to the sensing hardware itself. Ongoing risks result from fragmented ownership, weak interoperability requirements, discontinuous asset and data records, the late incorporation of security measures, unplanned software evolution and the lack of retirement plans. The Saudi studies also show that technology performance should be linked to governance, to the requirements of the end-users and to lifecycle appraisal, rather than being considered as an independent indicator of smartness. The paper introduces a Lifecycle Assurance Framework for Urban IoT, which connects each stage to decision gates, evidence artifacts and indicators. The framework regards product lifecycle management as the continuity layer that links devices, software, data, service outcomes and circularity. It provides a research-based foundation for procuring scalable urban IoT, for managing the associated operational changes and for reducing lifecycle risk in Saudi smart-city initiatives.

1. INTRODUCTION

Smart-city initiatives are now relying more and more on Internet of Things (IoT) products in order to detect conditions, transmit events and aid decision-making in a variety of areas such as transport, water, buildings, energy, safety and the environment. Recent reviews have outlined an ecosystem that includes sensors, networks, cloud or edge computing, analytics and service applications, while highlighting the ongoing difficulties concerning interoperability, security, scalability and data management [7-10]. Although this multi-layered technical perspective is necessary, it fails to account for the fact that a successful pilot still continues to deliver value even after thousands of different kinds of devices have been installed, upgraded, replaced and integrated with the municipal platforms. A smart-city technology is not a one-off purchase; it develops into an evolving product-service asset whose physical components, embedded software, identities, data models, analytics and service obligations undergo changes at different speeds.

It is important in Saudi Arabia that smart and sustainable city initiatives should be linked to broader aims of urban transformation. Research carried out in Saudi Arabia indicates that successful implementation involves more than just the use of advanced technology; lifecycle-based evaluation, coordination with stakeholders, meeting end-user requirements, governance and the alignment of the various initiatives are key factors affecting the quality of implementation [1,3-6]. In the case of Riyadh, a lifecycle approach has been used to connect the stages of conceptualisation, planning and design with those of installation or closure, involving stakeholders, setting key performance indicators and defining deliverables [1]. Other studies conducted in Saudi Arabia have stressed the role of urban computing and citizen involvement in turning technical capability into useful and acceptable services [4,5]. These results suggest that the deployment of IoT should be managed as a continuous lifecycle rather than as a process involving procurement and then installation; they also provide a basis for comparing projects that make use of different technologies but which rely on similar lifecycle controls.

Product lifecycle management (PLM) is a useful approach since it emphasizes information continuity, configuration control, traceability, and coordinated decision-making throughout a product's life. Digital-twin research builds on this idea by connecting physical entities to dynamic virtual representations and lifecycle data, while acknowledging that the usefulness of a

twin depends on model fidelity, data consistency, and maintenance [15-21]. In the case of a smart city, however, the relevant 'product' is wider than just a device; it also encompasses firmware, connectivity profiles, security credentials, data schemas, edge or cloud services, analytical models, application interfaces, maintenance history, service expectations and eventual reuse or disposal. If only the hardware is managed, then important dependencies will lie outside the scope of managerial control.

The literature is still scattered throughout the areas of technical architecture, cyber risk, digital twins, sustainability and smart-city governance. Although reviews cover the IoT technologies and the associated challenges [7-10,30], they seldom arrange the knowledge relating to deployment in terms of decisions made throughout the product lifecycle. While studies on PLM and digital twins do offer concepts concerning the lifecycle, they are mostly based on manufacturing and industrial assets [15-18]. The Saudi smart-city studies focus on implementation and participation, but do not fully explain how device configuration, data continuity, security evolution and retirement should be managed within an urban technology portfolio [1,3-6]. The practical outcome is that a city might approve a sensor network without deciding who is responsible for maintaining its software inventory, verifying updates, preserving semantic interoperability, measuring energy use or retiring outdated devices without losing the historical context.

Therefore, this review seeks to explore how the principles of PLM can enhance the deployment of IoT-enabled smart city technologies in Saudi Arabia. Its purpose is to combine technical and managerial evidence into a lifecycle assurance model, covering the entire period from problem definition to the end of the technology's life. The analysis is guided by four objectives: identifying the failure points that are specific to each stage of the lifecycle; linking the technical, governance and sustainability controls to these failure points; interpreting the evidence in the context of Saudi urban initiatives; and suggesting measurable stage gates which will help to maintain value, trust and adaptability. This contribution is not a generic smart city architecture. Instead, it is a governance-focused synthesis that explains what kind of evidence should exist,

when it should be reviewed, and how ensuring lifecycle continuity can reduce the gap between a successful demonstration and a reliable city-wide service.

2. CONCEPTUAL FOUNDATION: FROM IOT ARCHITECTURE TO PRODUCT LIFECYCLE

A typical IoT architecture breaks down a service into its sensing, communication, processing and application components. Surveys carried out in the context of smart cities show different versions of this structure, with arrangements such as cloud, fog and edge being chosen on the basis of latency, privacy, resilience and resource constraints [7,8,14,26]. The wastewater study referred to offers a specific example: edge processing is carried out using the sensors and data collection, together with cloud services and application-level monitoring, and blockchain is employed for validation and traceability [2]. The drawback of such an approach is that it is temporal in nature; it explains where processing takes place rather than detailing how a city should manage a device from the stage of requirements definition through to upgrades, ownership transfers and retirement.

PLM includes a temporal element. It connects requirements, design decisions, configurations, operating evidence and changes. The principle is made clear in the literature on digital twins: twins rely on reliable mappings between physical assets, models and lifecycle data, and these mappings have to endure modification [15-18]. Studies of urban digital twins also claim that city-wide representations can aid governance, scenario analysis, feedback and decision support, but their value is dependent on data quality, interoperability and a continued link with physical systems [19-22]. With regard to IoT, lifecycle integrity means that five questions can be answered at any given time—what asset has been deployed, why it exists, how it is configured, what evidence shows that it performs safely and usefully, and what dependencies must be protected when it changes.

It therefore follows that the appropriate unit for lifecycle management should be the configuration of an IoT product-service rather than a single sensor. A field device might be technically working when in fact the service has failed since its certificate has expired, the protocol version is not supported, the calibration history is unknown, the data schema has changed without notice, or the analytics model no longer matches the present conditions. Research into security supports this approach which takes the system as a whole. In the case of smart cities, urban data is centralised and vulnerabilities can spread via mobile devices, gateways, networks, platforms and third-party services [11-13]. Security cannot be introduced after deployment because identity, the mechanisms for updating, data minimisation, access control and evidence of incidents are design features that must be kept under control throughout the lifecycle.

The way in which lifecycle thinking is understood also alters the interpretation of sustainability. Research into green-IoT indicates that the smart-city technologies in question cause environmental burdens as a result of the energy used by the devices, the demand on networks and computing resources, the materials employed and the electronic waste produced [24,25]. Scholarship concerning e-waste shows the importance of using life-cycle assessment and material-flow analysis if one is to understand the stocks and flows of materials, the recovery processes and the associated environmental impacts [29]. A city which improves the energy it uses but at the same time replaces its devices too early may end up transferring the burden rather than reducing it. Lifecycle governance should therefore take into account, together with operational efficiency, such factors as maintainability, repairability, the longevity of components, compatibility with upgrades, the possibility of reuse and responsible recovery.

The situation in Saudi Arabia involves certain institutional and social demands. Studies carried out within the Kingdom indicate that coordinated governance, the involvement of stakeholders, and the establishment of implementation frameworks which connect strategy with specific projects are all necessary [1,4,5]. Research involving end users demonstrates that the socio-organisational, financial and technical requirements should influence the design of the IoT architecture rather than being treated only as issues that arise later during adoption [3]. Findings

from research into citizen acceptance also reach this same conclusion, namely that trust and social influence can have a significant effect on the use of sustainable services that are enabled by IoT [23]. Success in putting such initiatives into practice must therefore be defined by the continued provision of the intended public value despite acceptable levels of technical, cyber, financial, environmental and social risk. While the installation phase is an important achievement, it is by no means the final stage.

The six lifecycle stages that are used in this review are: the definition of value and the development of a concept; architecture, design and procurement; integration and commissioning; operation and maintenance; upgrade, scaling and reconfiguration; and retirement, reuse or recycling. These stages are more comprehensive than a hardware lifecycle since urban IoT involves both physical and digital assets. In all the stages, the analysis makes use of six assurance dimensions: governance and accountability; interoperability and data continuity; cybersecurity and privacy; service performance and resilience; user and stakeholder value; and environmental circularity. The stages together with the dimensions form the analytical framework for interpreting the evidence and for constructing the proposed framework.

3. REVIEW METHODOLOGY

A structured integrative review was used since the research question spans the fields of engineering, information systems, urban governance, and sustainability and so cannot be answered using the evidence from a single discipline. The time frame for the review was from January 2020 to December 2025, which corresponds to the period specified for the manuscript and also includes recent work in the areas of smart-city IoT and lifecycle studies. The potential studies were found by combining terms such as "Internet of Things", "IoT", "smart city", "Saudi Arabia", "lifecycle", "product lifecycle management", "digital twin", "interoperability", "cybersecurity", "edge computing", "citizen acceptance", "green IoT" and "e-waste". Preference was given to peer-reviewed journal articles that were indexed in major scholarly databases,

although one peer-reviewed conference paper was included because it directly deals with IoT device lifecycle management [28].

To be eligible, a publication had to have been issued between 2020 and 2025, come from an English-language scholarly source, have a verifiable digital object identifier (DOI), and be substantially relevant to at least one lifecycle stage or assurance dimension. Publications were excluded if they were mainly promotional, failed to provide evidence of having been peer-reviewed, did not have a DOI, or if they dealt with a narrow algorithm without any implications for deployment, lifecycle control or the Saudi smart-city context. Thirty publications made up the final set of evidence. Before being included, the DOI strings and bibliographic metadata were verified against records from the publisher, indexing service or the institution in question. The two papers that were uploaded were regarded as anchor references since they respectively deal with lifecycle-based smart-city implementation in Riyadh [1] and with an IoT smart-city architecture incorporating sensors, edge computing, cloud services and blockchain functions [2].

The analysis carried out two stages of coding. During the first stage, each study was coded according to its main contribution—this could be implementation governance, architecture, sensor deployment, data and interoperability, cybersecurity and privacy, edge intelligence, digital twins, user acceptance, sustainability or end-of-life. In the second stage, the findings were assigned to the six lifecycle phases and the six assurance dimensions previously defined. A finding was kept only if it referred to a deployment requirement, a recurring problem, a control mechanism, a decision criterion or a measurable outcome. With this method, it was possible to compare evidence from different areas at the point in the lifecycle when it had managerial significance.

The review is not a meta-analysis but an interpretive one. The studies cited employ a variety of methods, units of analysis and outcome measures, so combining their numerical results would give a misleading impression of comparability. Rather, the synthesis concentrates on convergence, tension and dependency. For instance, reviews of architecture consistently point

out interoperability and scalability as open challenges [8-10,30], whereas security reviews highlight privacy and attack exposure [11-13]. The digital-twin studies identify the need for persistent data-model correspondence [15-22], and the sustainability studies extend lifecycle responsibility to include energy and material flows [24,25,29]. The approach thus does not ask "which technology scores highest?" but instead asks "which lifecycle decisions are repeatedly necessary for technologies to remain deployable, trustworthy and valuable?" Figure 1 presents the review logic.

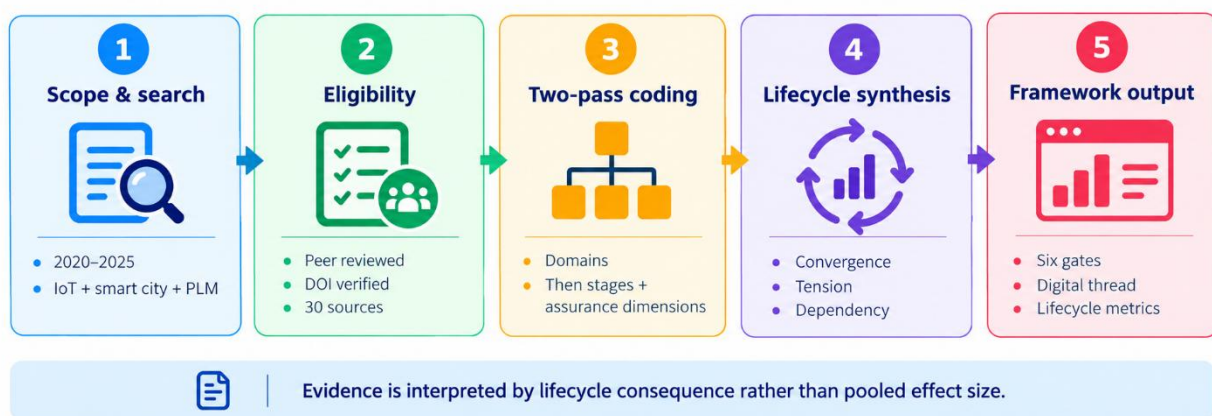


Figure 1. Structured integrative review and synthesis workflow used in this study.

4. EVIDENCE SYNTHESIS

4.1 Value definition, requirements and portfolio selection

The first risk in the lifecycle comes about prior to a sensor being chosen. As Saudi evidence indicates, the quality of implementation is determined by linking projects to strategic objectives, to stakeholders and to measurable outcomes [1,4,5]. A programme that is managed over its lifecycle should therefore start with a service problem and a value hypothesis—that is, what urban condition should be improved, who the people are who experience the problem, what decision will be enabled by IoT data, and which outcome will serve as a justification for

continuing the programme? Thus traceability can be established from public value to technical requirement.

The conditions under which value could fail also have to be included in the requirements. Alreshidi and Alyami [3] show how important it is to have socio-organisational, financial and technical end-user requirements when developing smart cities in Saudi Arabia, and acceptance studies point to trust as a key factor in the use of IoT-based sustainable services [23]. The concept gate should therefore take into account stakeholder ownership, acceptable data use, operational response capacity and lifecycle cost, not just sensing accuracy. A city must avoid gathering data unless it has established who is authorised and who has the resources to take action on it.

When putting together a portfolio it is necessary to record information regarding coverage, connectivity, robustness, lifetime and the budget assumptions. Research into sensor deployment in Saudi Arabia demonstrates that these objectives conflict with one another [6]. Since urban form, demand and network topology are all subject to change, the reasons for the placement decisions must be kept. The implication for PLM is simple: traceability from requirements to configuration should start before any procurement takes place.

4.2 Architecture, procurement and interoperability by design

It is in the field of architecture that flexibility over the product's lifecycle is either achieved or limited. Smart-city IoT systems usually involve sensing, networking, edge or fog processing, as well as cloud services and applications [7,8], but examinations of various frameworks show that interoperability, scalability and sustainability are only partly dealt with [9,30]. These aspects should therefore be included as requirements in procurement processes together with testable acceptance criteria rather than treated as goals.

Interoperability involves many different levels: devices have to be able to connect, the messages have to be readable in terms of their structure, the data has to keep the same meaning across systems, and the organisations themselves have to co-ordinate any changes. Similarly, research focused on blockchain points out that standardisation and cross-node interoperability are still unresolved issues in the context of smart cities [27]. Lifecycle specifications should therefore include requirements for stable identifiers, documented APIs, versioned schemas, exportable data, rules for time synchronisation, records of configuration and obligations regarding change notification. It is still possible to use proprietary technology, but lock-in will then be obvious and can be managed.

Procurement ought to distinguish between the outcomes of a service and the decisions regarding its implementation. The wastewater study referenced makes use of sensors, gateways, edge processing, cloud functions and blockchain-supported validation [2]. The key lesson that can be applied elsewhere is not that all services need blockchain; rather, responsibilities for sensing, validation, processing, storage and decision support must be made explicit. Although edge processing can reduce latency, bandwidth and the exposure of raw data, it does so at the cost of introducing resource and orchestration constraints [14,26]. Workload placement, disconnected operation and distributed software updating should therefore be specified before any purchase is made.

Cybersecurity and privacy should likewise be considered as part of the entire lifecycle. The reviews cover the risks associated with devices, networks, infrastructure and services [11-13]. Evidence relating to the design should include aspects concerning identity, the provisioning of credentials, encryption, least-privilege access, logging, how vulnerabilities are dealt with, the support periods, key rotation and decommissioning. Since vulnerabilities appear after commissioning, the supplier's ability to provide support for secure changes should affect procurement decisions.

4.3 Integration, commissioning and evidence-based acceptance

280

281 The integration of products into a city service should be viewed as an evidence gate; although
282 individual components may pass their separate tests, they can still fail when put together due to
283 clock drift, conflicting schemas, changes in radio conditions, divergence in platform policies or
284 because the operators are unprepared. The evidence required for commissioning therefore ought
285 to incorporate architecture, sensor, edge and security measures [6,9,11-13,26]. A practical
286 evidence pack should include as-built asset records, the software versions, the interface tests, the
287 calibration baselines, the coverage results, the resilience tests, the security verification and the
288 data-quality thresholds together with operator acceptance.

289

290 Data lineage is important since later users might not know which device, calibration state,
291 firmware, transformation or model was responsible for a historical observation. Research into
292 digital twins identifies the existence of a consistent relationship between physical entities,
293 models and data as a fundamental requirement [15-18], and studies of city twins demonstrate
294 how various urban systems rely on reliable data links [19-21]. When commissioning is carried
295 out, persistent asset identifiers should be created and metadata should be used to link the
296 observations to the source configurations; otherwise, although the historical data can still be
297 accessed it will lose its operational meaning.

298

299 Acceptance testing should include the various degraded states such as loss of connectivity,
300 gateway failure, sensor values that are implausible, cloud interruption, or a change in the third-
301 party interface. The IoT-WMS study shows how anomaly detection and combined edge-cloud
302 processing can be used for abnormal data [2]. More broadly speaking, cities should have clearly
303 defined alert ownership and response procedures, not just dashboards which only display faults.

304

305 4.4 Operation, maintenance and the living configuration

306

Once it has been commissioned, the IoT system forms a changing installed base since the batteries wear out, calibration tends to drift, certificates expire, updates and new models come out. Viewing the original as-built design as final results in configuration debt; instead, PLM calls for a living record in which material changes cause the asset status to be updated and lead to a reappraisal of the affected controls.

The literature on digital twins and maintenance backs up this principle by showing how physical condition, models, and operational data are linked [16-18]. In the case of urban IoT, the most useful twin would be a simple version that accurately keeps record of identity, location, configuration, health, dependencies, and change history rather than a visually detailed model which has a poor maintenance routine. Service monitoring should also go further than just checking device availability. A sensor that is online can still provide biased data; a network that is available may yet be too slow; and an analytics model can lose accuracy over time. Useful indicators should include data completeness, compliance with calibration, decision latency, false alarms, maintenance burden, and service outcomes [14,26].

Security operations must use the same lifecycle record; replacements, new interfaces, credential renewal and vendor changes all affect the attack surface [11-13]. By linking firmware status, credentials, network relationships, data classification and support status to the level of service criticality, risk-based patching and incident response can be carried out.

It is important to give special consideration to operational data governance since the urban IoT produces records which can last longer than the lifetime of the device and be used again for planning, analytics or as regulatory evidence. As a result, data retention must be based on its purpose, level of sensitivity and reproducibility rather than on the principle of unlimited storage. Any changes to units, schemas, filtering rules or calibration methods should be versioned so that analysts will be able to reconstruct how a value was obtained. This need links interoperability with accountability in that a dataset which is technically accessible cannot be reused if there is uncertainty about its semantics or provenance. Moreover, persistent metadata reduces reliance on

individual suppliers by enabling authorised teams to interpret historical information even when the platforms or contracts have changed.

4.5 Upgrade, scaling and controlled evolution

Scaling brings to light underlying assumptions. Adding more nodes leads to greater demands in terms of key management, network congestion, data volume, the need for maintenance, and reliance on suppliers; scalability and adaptability remain major challenges [9,10,30]. When expanding, there must be a clear stage passed which involves capacity tests covering the network, the edge, the cloud, storage, analytics and support operations, as well as ensuring semantic compatibility in the case of the introduction of new device types or vendors.

In any instance where machine learning is applied, model governance must specify the training provenance, the validation process, drift monitoring, rollback procedures, and the relationships between different model versions and the assets they affect. Research into federated learning and digital twins shows promise in terms of preserving privacy through distributed intelligence while still facing trust and integration challenges [22]. Hardware, firmware and models should therefore be subject to a single change-control procedure. Prior to a rollout, an impact analysis had better identify the dependencies; the deployment should be carried out in stages, with it being possible to observe the results and reverse the changes if necessary. A digital thread based on PLM principles makes it possible to discover those dependencies before any change reaches city scale.

The process of switching suppliers is yet another test of a system's lifecycle. Since smart-city initiatives often combine equipment and services that have different lengths of commercial support, obsolescence can occur even if the hardware itself is still working. Therefore, before scaling up, owners must identify components that depend on a single source, use unsupported libraries, have expiring licences or involve proprietary interfaces and establish ways to substitute

364 them. When assessing proposed upgrades, change boards should not just check whether the
365 upgrade functions, but also whether it affects the future portability, maintenance capability or the
366 ability to retain evidence. In this way, adaptability becomes a property that is governed rather
367 than taken for granted. This kind of evidence allows the difference between a planned renewal
368 and one that is caused by lifecycle failures to be identified.

370 4.6 Retirement, circularity and preservation of public value

372 Even when city programmes may end up with a large number of devices, end-of-life is
373 frequently not clearly defined. Research into Green-IoT connects connected technology with
374 energy demand, material usage and e-waste [24,25], and studies of e-waste demonstrate how life-
375 cycle assessment and material-flow analysis can show recovery possibilities and environmental
376 impacts [29]. Before deployment, retirement must be defined, with attention to service migration,
377 data preservation, the revocation of credentials, storage sanitisation, component reuse and
378 material recovery.

380 The context necessary for interpreting historical records should not be deleted when a device is
381 removed. After the physical recycling of a device, the metadata relating to identity, location,
382 service period, calibration and configuration should be retained, while secrets and personal data
383 must not be left recoverable on the hardware. Purchasing decisions should also take circularity
384 into account by considering factors such as modularity, the use of replaceable power systems, the
385 length of support offered and the documented material composition, as these can all help to
386 extend the device's useful life. The total cost of a device's lifecycle should cover maintenance
387 visits, energy usage, communications, computing, spares, software support and disposal. When
388 looking at the city level, the small individual impacts per device add up to significant overall
389 effects.

391 **Table 1. Evidence domains supporting lifecycle assurance for urban IoT.**

Evidence domain	Main synthesis	Lifecycle implication	Key refs
Saudi governance and participation	Strategy-project alignment, lifecycle appraisal and stakeholder involvement are implementation conditions.	Define value, owners and decision rights before technical selection.	[1,3-5]
IoT architecture and deployment	Layered sensing, network, edge/cloud and application functions face coverage, interoperability and scalability trade-offs.	Specify testable interfaces, placement assumptions and support constraints.	[2,6-10,30]
Cybersecurity and privacy	Risk spans devices, networks, platforms and services, and changes after commissioning.	Design identity, updates, logging, privacy and decommissioning as lifecycle controls.	[11-13]
Edge intelligence and analytics	Latency and privacy benefits depend on resource, orchestration and data-quality constraints.	Govern workload placement, models, drift, rollback and distributed updates.	[14,26]
Digital twins and lifecycle data	Value depends on persistent correspondence among physical assets, models and lifecycle evidence.	Maintain identifiers, configuration history, lineage and dependency records.	[15-22,28]
Sustainability and circularity	Energy, material use and e-waste extend responsibility beyond operational efficiency.	Include support life, repair, reuse, sanitisation and verified recovery.	[24,25,29]

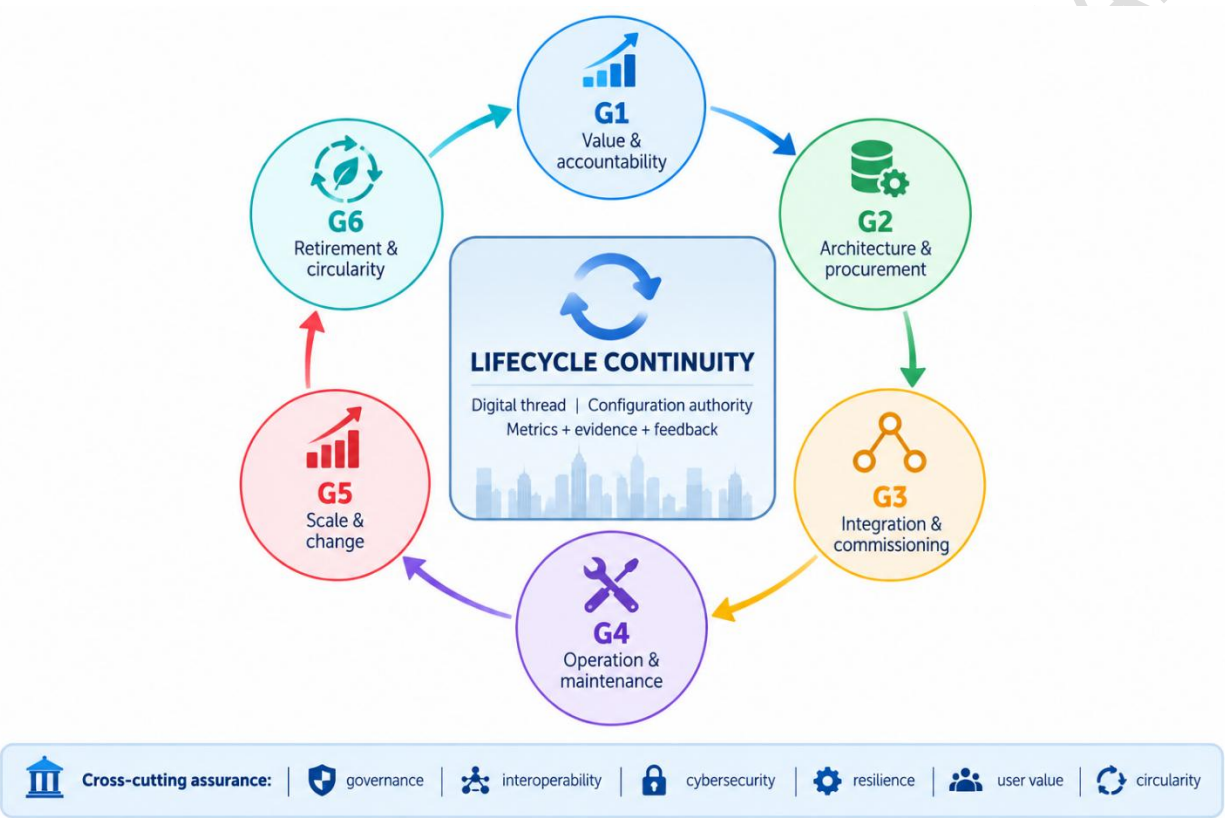
392

393 **5. LIFECYCLE ASSURANCE FRAMEWORK FOR URBAN IOT**

394

395
396
397
398
399

The synthesis offers a Lifecycle Assurance Framework for Urban IoT (LAF-UIoT) which is intended for use in Saudi smart-city programmes. The key idea behind it is evidence continuity, since the artefacts produced at each stage of the lifecycle serve as controlled inputs for the following stage, and operational evidence can cause earlier assumptions to be re-evaluated. Figure 2 shows the framework and Table 2 converts it into stage gates.



400

401 Figure 2. Lifecycle Assurance Framework for Urban IoT

402 Table 2. Proposed lifecycle stage-gate matrix for Saudi smart-city IoT products.

Gate	Decision question	Required evidence / control	Indicative metrics
G1 Value & accountability	Is the service problem, public value and accountable owner clear?	Value case; stakeholder map; data purpose; lifecycle budget; success criteria.	Outcome baseline; owner coverage; acceptance criteria completeness.

Gate	Decision question	Required evidence / control	Indicative metrics
G2 Architecture & procurement	Can the solution evolve securely without losing interoperability?	Interface/schema specifications; security architecture; update/support commitments; exit and retirement clauses.	Interface conformance; supported-life coverage; portability risk.
G3 Integration & commissioning	Does the integrated service perform under normal and degraded conditions?	As-built register; calibration; resilience/security tests; lineage metadata; operator acceptance.	Coverage; latency; completeness; calibration pass rate; recovery tests.
G4 Operation & maintenance	Is the living configuration known and is service value sustained?	Asset/dependency register; incidents; patches; maintenance; model versions; service outcomes.	Availability; patch latency; MTTR; false alarms; data quality; user value.
G5 Scale & controlled change	Can change be introduced without breaking service, trust or evidence continuity?	Impact analysis; capacity and compatibility tests; staged rollout; rollback; model governance.	Change success; rollback readiness; capacity margin; unsupported variants.
G6 Retirement & circularity	Can service be closed or migrated without residual cyber, data or material risk?	Migration plan; archive rules; credential revocation; sanitisation; reuse/recovery records.	Sanitisation verification; reuse/recovery rate; service life; early-replacement causes.

403

404 At Gate 1 value and accountability are set up. The sponsoring organisation specifies the urban
405 problem, the desired service outcome, who the affected stakeholders are, the purpose of the data,

the person responsible for decisions, the budget for the whole lifecycle and the measurable criteria for success. This is in keeping with Saudi research which stresses implementation governance, lifecycle appraisal and participation [1,4,5]. A concept should not move forward just because funding or technology is available; it had better explain how the data will support a decision that is owned by the organisation.

Gate 2 sets up an architecture that can evolve. The requirements are turned into specifications concerning interface, security, performance, support and circularity. The baseline consists of asset identifiers, data models, APIs, a credential architecture, mechanisms for updates, rules regarding the placement of edge and cloud resources, the expected support life and the obligations concerning retirement. The aim is not to get rid of vendor diversity but to make sure that this diversity remains manageable. Evidence from studies on frameworks and standardisation treats interoperability as a requirement throughout the lifecycle and not as something to be addressed after integration [9,27,30].

The integrated service is accepted at Gate 3 on the basis of the evidence. During commissioning, confirmation is given regarding coverage, calibration, latency, resilience, data lineage, security configuration, operator readiness and behaviour in degraded mode. As a result, a complete digital record is produced, not merely a signed installation certificate. At Gate 4 control of operations is exercised via a living register of assets and dependencies. Information relating to maintenance, incidents, patches, calibration, performance and user outcomes is fed into the record, which in turn allows for prioritised decisions. The digital-twin principles help to ensure this continuity when they are implemented as reliable links between the physical state and the lifecycle information [15-21].

Gate 5 is responsible for dealing with scale and changes; the proposed upgrades are examined in terms of their interoperability, security, capacity, effect on the model, supportability and the possibility of rollback. The key issue is whether the change maintains the service contract and the evidence chain. Scaling will only be approved if the operational capabilities increase in line

with the number of devices. Gate 6 brings the lifecycle to a close by ensuring secure retirement, migrating the service, preserving the historical data, revoking the credentials, carrying out sanitisation, enabling reuse and carrying out responsible material recovery. Environmental indicators should be reported together with the service and financial outcomes [24,25,29].

The gates are linked by three mechanisms. The first of these is a digital thread which ensures that there is a traceable record relating to requirements, assets, configuration, data and changes. The second is configuration authority, which specifies who is authorised to approve technical and service changes across different parts of the organisation. The third is the use of lifecycle metrics, which make degradation apparent. A set of practical indicators includes the percentage of assets that have a known owner and support status; interface conformance; patch latency; data completeness; calibration compliance; mean time to restore service; energy used per useful observation or transaction; user-service acceptance; the percentage of changes that have rollback evidence; and the percentage of retired assets that have had their data sanitised and their recovery disposition verified.

The framework makes a deliberate distinction between assurance and centralisation. The smart-city services in Saudi Arabia may be managed by various authorities, concessionaires and technology providers. LAF-UIoT does not demand that a single platform should have control over all devices; instead it calls for interoperable evidence regarding ownership, configuration and dependencies so that organisations which are distributed among different entities can co-ordinate decisions about the lifecycle of the services. This approach is in line with the literature which indicates that the implementation of smart cities is both a technical and an institutional process [1,4,30] and it also addresses a typical procurement risk, which is the transfer of operational dependence to a supplier without at the same time retaining enough information to govern change.

Table 1 brings together the evidence domains that support the framework; this pattern is seen in different bodies of literature. In the field of architecture, the question is whether the components

can work together and can be scaled up; in security studies, the issue is whether trust endures when things are exposed and changed; in those concerned with digital twins, the question is whether the physical and digital states stay synchronised; in acceptance studies, the question is whether the services remain useful and trusted; and in sustainability studies, the question is whether operational benefits are achieved without there being unmanaged energy and material consequences. PLM is the integrating discipline since each of these questions calls for reliable lifecycle information and controlled decisions.

6. DISCUSSION AND IMPLICATIONS

The review alters the meaning of "successful deployment": a project may be completed on time yet still be deficient from a lifecycle point of view if there is uncertainty about future patching, the data semantics cannot be preserved, maintenance ownership is not clear, or there is no established procedure for retirement. On the other hand, an architecture containing fewer new components could generate greater public value if it is observable, supportable and adaptable. This difference is important for the Saudi programmes since their scale, the speed of urban development and the involvement of multiple entities can increase the complexity of configuration and governance [1,4,5].

For those who are public owners, the main point is to obtain evidence of the product's entire lifecycle rather than just the devices themselves. The terms of the tender should request that bidders show that they provide update support, have governance over interfaces, ensure data portability, maintain asset identity, deal with vulnerabilities, offer configuration exports, have a spares strategy and carry out retirement procedures. When assessing the proposals, account should be taken of the total lifecycle cost as well as the cost involved in changing the supplier or platform. Contracts must assign responsibility for records, not just for carrying out maintenance activities, since the absence of such records makes it expensive or even impossible to give later assurance.

492

493 For technology companies, PLM provides an opportunity to stand out by focusing on
494 maintainability and transparency. The use of standard interfaces, documented dependencies,
495 secure channels for updates, and exportable records of the product's lifecycle all help to reduce
496 the difficulties involved in integrating systems. Although edge intelligence and digital twins can
497 provide a great deal of value, this is only the case when their own models and software are
498 versioned and linked to operational evidence [16,21,26]. Having sophisticated systems without a
499 strict configuration process actually increases rather than decreases the risk during the product's
500 lifecycle.

501

502 For researchers the framework indicates that assessment should go beyond relying on single-
503 stage performance measures. Most studies currently give figures for accuracy, latency, coverage
504 or energy use under controlled conditions. Future demonstrations in Saudi Arabia should also
505 include information on upgrade effort, interoperability between versions, support workload,
506 security response, the continuity of data lineage, user acceptance and the outcomes at the end of
507 a system's life. Incorporating these factors would make the research more comparable with the
508 long-term decisions that city operators have to make.

509

510 The stage-gate approach also provides a practical link between urban governance and
511 engineering. In governance, it is established who is responsible and what kind of public outcome
512 is acceptable; in engineering, it is decided how sensing, communication, computation and control
513 enable that outcome. The digital thread joins the two by retaining the reason for an asset's
514 existence and showing how evidence regarding its behaviour changes over time. Lifecycle
515 management is therefore not merely administrative overhead; it is the means by which technical
516 capability remains in line with the service objective for which public resources were allocated.

517

518 7. LIMITATIONS AND FUTURE RESEARCH

519

There are three limitations to this review. The first is that it brings together different kinds of evidence rather than calculating an overall effect; the relationships suggested therefore need to be tested through empirical research. The second is that the boundary set between 2020 and 2025 gives a bias in favour of more recent technologies and excludes earlier foundational work in the areas of PLM and IoT. The third is that there is still a lack of Saudi-specific empirical studies covering the full IoT lifecycle, which means that some of the controls have been taken from research on smart cities and digital twins and thus require validation in the context of Saudi Arabia.

Future research should involve the testing of LAF-UIoT using longitudinal case studies conducted in Saudi Arabia, the studies covering the procurement phase, the commissioning phase, various update cycles and the retirement phase. A comparative study could look at whether the level of maturity at each lifecycle gate is associated with service availability, cyber response time, total cost, citizen trust or environmental performance. There is also a need for research into machine-readable lifecycle records that link together municipal asset systems, digital twins and supplier data without requiring the use of a single proprietary platform. Lastly, lifecycle carbon and material indicators should be combined with service-value metrics so that environmental efficiency can be evaluated on a per-useful urban outcome basis rather than on a per-device basis.

8. CONCLUSION

Smart-city services can only be realised through the use of connected products that stay trustworthy, interpretable, maintainable and valuable as they change. Evidence obtained between 2020 and 2025 indicates that interoperability, cybersecurity, data continuity, operational support, user trust and environmental responsibility are lifecycle dependencies and not merely separate technical features. Further research carried out in Saudi Arabia shows that governance, participation and a staged approach to implementation are also important. The proposed LAF-UIoT framework combines all these elements using six lifecycle gates, a continuous digital

thread and cross-cutting assurance metrics. Its main idea is simple: cities should treat IoT as evolving product-service configurations rather than as fixed hardware. This approach can lead to better procurement quality, stronger commissioning evidence, more effective change control, greater operational resilience and more responsible retirement, thus providing Saudi smart-city programmes with a clearer foundation on which to scale their technology without having to scale unmanaged lifecycle risk.

References

1. Alshuwaikhat HM, Adenle YA, Almuhaideb T. A Lifecycle-Based Smart Sustainable City Strategic Framework for Realizing Smart and Sustainability Initiatives in Riyadh City. Sustainability. 2022;14(14):8240. <https://doi.org/10.3390/su14148240>
2. Alzahrani AIA, Chauhdary SH, Alshdadi AA. Internet of Things (IoT)-Based Wastewater Management in Smart Cities. Electronics. 2023;12(12):2590. <https://doi.org/10.3390/electronics12122590>
3. Alreshidi E, Alyami SH. End-users' requirements underpinned by IoT layered architecture to the development of smart sustainable cities. The Journal of Engineering. 2020;2020(11):1065-1073. <https://doi.org/10.1049/joe.2019.1258>
4. Alshuwaikhat HM, Aina YA, Binsaedan L. Analysis of the implementation of urban computing in smart cities: A framework for the transformation of Saudi cities. Heliyon. 2022;8(10):e11138. <https://doi.org/10.1016/j.heliyon.2022.e11138>
5. Alamoudi AK, Abidoye RB, Lam TYM. Implementing Smart Sustainable Cities in Saudi Arabia: A Framework for Citizens' Participation towards SAUDI VISION 2030. Sustainability. 2023;15(8):6648. <https://doi.org/10.3390/su15086648>
6. Alablani I, Alenazi M. EDTD-SC: An IoT Sensor Deployment Strategy for Smart Cities. Sensors. 2020;20(24):7191. <https://doi.org/10.3390/s20247191>

- 575 7. Syed AS, Sierra-Sosa D, Kumar A, Elmaghraby A. IoT in Smart Cities: A Survey of
576 Technologies, Practices and Challenges. *Smart Cities*. 2021;4(2):429-475.
577 <https://doi.org/10.3390/smartcities4020024>
- 578 8. Bellini P, Nesi P, Pantaleo G. IoT-Enabled Smart Cities: A Review of Concepts, Frameworks
579 and Key Technologies. *Applied Sciences*. 2022;12(3):1607. <https://doi.org/10.3390/app12031607>
- 580 9. Peralta Abadia JJ, Walther C, Osman A, Smarsly K. A systematic survey of Internet of Things
581 frameworks for smart city applications. *Sustainable Cities and Society*. 2022;83:103949.
582 <https://doi.org/10.1016/j.scs.2022.103949>
- 583 10. Rejeb A, Rejeb K, Simske S, Treiblmaier H, Zailani S. The big picture on the internet of
584 things and the smart city: a review of what we know and what we need to know. *Internet of*
585 *Things*. 2022;19:100565. <https://doi.org/10.1016/j.iot.2022.100565>
- 586 11. Ismagilova E, Hughes L, Rana NP, Dwivedi YK. Security, Privacy and Risks Within Smart
587 Cities: Literature Review and Development of a Smart City Interaction Framework. *Information*
588 *Systems Frontiers*. 2022;24(2):393-414. <https://doi.org/10.1007/s10796-020-10044-1>
- 589 12. Hernandez-Ramos JL, Martinez JA, Savarino V, Angelini M, Napolitano V, Skarmeta AF,
590 Baldini G. Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and
591 Future Directions. *IEEE Security & Privacy*. 2021;19(1):12-23.
592 <https://doi.org/10.1109/MSEC.2020.3012353>
- 593 13. Ogonji MM, Okeyo G, Wafula JM. A survey on privacy and security of Internet of Things.
594 *Computer Science Review*. 2020;38:100312. <https://doi.org/10.1016/j.cosrev.2020.100312>
- 595 14. Ben Atitallah S, Driss M, Boulila W, Ben Ghezala H. Leveraging Deep Learning and IoT big
596 data analytics to support the smart cities development: Review and future directions. *Computer*
597 *Science Review*. 2020;38:100303. <https://doi.org/10.1016/j.cosrev.2020.100303>
- 598 15. Jones D, Snider C, Nassehi A, Yon J, Hicks B. Characterising the Digital Twin: A systematic
599 literature review. *CIRP Journal of Manufacturing Science and Technology*. 2020;29:36-52.
600 <https://doi.org/10.1016/j.cirpj.2020.02.002>

16. Lim KYH, Zheng P, Chen CH. A state-of-the-art survey of Digital Twin: techniques, engineering product lifecycle management and business innovation perspectives. *Journal of Intelligent Manufacturing*. 2020;31(6):1313-1337. <https://doi.org/10.1007/s10845-019-01512-w>
17. Liu M, Fang S, Dong H, Xu C. Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems*. 2021;58(B):346-361. <https://doi.org/10.1016/j.jmsy.2020.06.017>
18. Errandonea I, Beltran S, Arrizabalaga S. Digital Twin for maintenance: A literature review. *Computers in Industry*. 2020;123:103316. <https://doi.org/10.1016/j.compind.2020.103316>
19. White G, Zink A, Codeca L, Clarke S. A digital twin smart city for citizen feedback. *Cities*. 2021;110:103064. <https://doi.org/10.1016/j.cities.2020.103064>
20. Deng T, Zhang K, Shen ZJ. A systematic review of a digital twin city: A new pattern of urban governance toward smart cities. *Journal of Management Science and Engineering*. 2021;6(2):125-134. <https://doi.org/10.1016/j.jmse.2021.03.003>
21. Wang H, Chen X, Jia F, Cheng X. Digital twin-supported smart city: Status, challenges and future research directions. *Expert Systems with Applications*. 2023;217:119531. <https://doi.org/10.1016/j.eswa.2023.119531>
22. Ramu SP, Boopalan P, Pham QV, Maddikunta PKR, Huynh-The T, Alazab M, Nguyen TT, Gadekallu TR. Federated learning enabled digital twins for smart cities: Concepts, recent advances, and future directions. *Sustainable Cities and Society*. 2022;79:103663. <https://doi.org/10.1016/j.scs.2021.103663>
23. Bestepe F, Ozkan Yildirim S. Acceptance of IoT-based and sustainability-oriented smart city services: A mixed methods study. *Sustainable Cities and Society*. 2022;80:103794. <https://doi.org/10.1016/j.scs.2022.103794>
24. Almalki FA, Alsamhi SH, Sahal R, Hassan J, Hawbani A, Rajput NS, Saif A, Morgan J, Breslin J. Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities. *Mobile Networks and Applications*. 2023;28(1):178-202. <https://doi.org/10.1007/s11036-021-01790-w>

25. Al-Obaidi KM, Hossain M, Alduais NAM, Al-Duais HS, Omrany H, Ghaffarianhoseini A. A Review of Using IoT for Energy Efficient Buildings and Cities: A Built Environment Perspective. *Energies*. 2022;15(16):5991. <https://doi.org/10.3390/en15165991>
26. Bourechak A, Zedadra O, Kouahla MN, Guerrieri A, Seridi H, Fortino G. At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. *Sensors*. 2023;23(3):1639. <https://doi.org/10.3390/s23031639>
27. Alasbali N, Azzuhri SRB, Salleh RB, Kiah MLM, Shariffuddin AAASA, Kamel NMIBNM, Ismail L. Rules of Smart IoT Networks within Smart Cities towards Blockchain Standardization. *Mobile Information Systems*. 2022;2022:9109300. <https://doi.org/10.1155/2022/9109300>
28. Georgalas N, Ennis A, Peoples C, Rafferty J, Perry P, Cristina C, Black B, Moore A, Bowman T, Scotney B, Reeves A. IoT Device Lifecycle Management. In: 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications. 2024:1865-1870. <https://doi.org/10.1109/TRUSTCOM60117.2023.00253>
29. Withanage SV, Habib K. Life Cycle Assessment and Material Flow Analysis: Two Under-Utilized Tools for Informing E-Waste Management. *Sustainability*. 2021;13(14):7939. <https://doi.org/10.3390/su13147939>
30. Omrany H, Al-Obaidi KM, Hossain M, Alduais NAM, Al-Duais HS, Ghaffarianhoseini A. IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction. *Discover Cities*. 2024;1:2. <https://doi.org/10.1007/s44327-024-00002-w>