Enhanced European Internet of Things (IoT) Platform Assessment Key Performance Indicators (KPIs)

Okta Nurika[1(✉)] and Low Tan Jung[2]

[1] HELP University, No. 15, Sri Semantan 1 Street, Off Semantan Street, Damansara Heights, 50490 Kuala Lumpur, Malaysia
okta.nurika@help.edu.my

[2] Computer and Information Sciences Department, Universiti Teknologi PETRONAS, 32610 Perak, Seri Iskandar, Malaysia
lowtanjung@utp.edu.my

Abstract. The current most established IoT platform assessment standard called CREATE-IoT is missing essential KPIs that cover both technical and business aspects. These new KPIs would enhance this standard and improve the quality of assessment outcomes, which eventually would encourage more IoT platform deployments worldwide and open more technology-related jobs that will drive the global economy upward. Through experiences in studying IoT platform technical architecture and business model, this paper formulates and adds 22 unique new KPIs to this standard that initially consists of 198 KPIs. Or conclusively, 11.11% of distinct enhancement has been made. Thus, now this enhanced version of CREATE-IoT assessment standard may cover more IoT platform elements than before.

Keywords: IoT · Platform · Assessment · KPI · CREATE-IoT

1 Introduction

Currently, there is only one known standard to assess Internet of Things (IoT) platform, which is the one developed by CREATE-IoT [1]; it is a set of evaluation methodologies and Key Performance Indicators (KPIs) based on a set of verifications. This standard has gained reputation as the standard used to assess IoT Large-Scale-Pilot projects in European countries. However, the KPIs in this standard are missing other essential KPIs that we have formulated. Therefore, this paper suggests additions and consolidations of more KPIs to be included into the original CREATE-IoT standard. Furthermore, these newly formulated KPIs would be normalized according to the existing categorization groups.

The author of this paper aspires to enhance the current CREATE-IoT assessment standard, because he has worked as an IoT platform assessment consultant for an Asian major telecommunication company. In the process, he had formulated additional assessment

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2021, LNICST 382, pp. 137–153, 2021.
https://doi.org/10.1007/978-3-030-78459-1_10

items that can complement this existing standard. Therefore, the area of IoT platform assessment would get significant enhancement.

Reference [1] categorizes IoT assessment items into eight dimensions or groups, which are Technology Development, Technology Deployment and Infrastructure, Ecosystem Strategy and Engagement, Ecosystem Openness and External Collaboration, Marketplace and Business Impacts, Societal and Economic Impacts, Policy and Governance Impacts, and Community Support and Stakeholders' Inclusion.

The review of these existing assessment dimensions above would become the basis of analyzing the missing or lacking KPIs.

2 IoT Platform Comparative Analysis

IoT platform assessment KPIs are based on the business and technical aspects that construct an IoT platform. There have been brief and simpler IoT platform assessments practices, which only cover the high level features and services of the platform – We prefer to call these comparative analysis instead of full assessment. These may offer quick insight into the platform's capabilities, however deeper assessment is needed to conclude the level of readiness and establishment of the platform. An example of comparative analysis was done by Paper [2], which assessed major IoT platform providers based on their capabilities and shortcomings. The results are presented in the next table (Table 1).

Table 1. Generic Major IoT Platform Assessments

Platform	Strength	Limitation
IBM IoT	Augmented reality, cognitive data processing, blockchain, edge analytics, natural language processing, integrated data sources (weather, maps, social media), pre-built apps (e.g., prescriptive maintenance)	Utilizing private cloud with limited set of public, private, & on-premises delivery options
C3 IoT	Predictive maintenance, inventory optimization, energy management, sensor health, fraud detection, supply network, CRM, anti-money laundering	Lacking augmented & virtual reality, steep learning curve at model-driven type system, less user-friendly UI
Microsoft	Comprehensive dev tools, advanced analytics capabilities, end-to-end security, broad set of open source tools, rich platform deployment options	Less pre-built apps compared to others, limited augmented reality capabilities
SAP Leonardo	Machine Learning, blockchain, analytics, big data, comprehensive industrial protocols, various pre-built apps	Confusing portfolio terminologies, limited device management functionality
PTC	Comprehensive device connectivity, comprehensive industrial connectivity protocols, comprehensive augmented reality use cases	Less user-friendly UI for device connectivity, limited tools for developers

(*continued*)

Table 1. (*continued*)

Platform	Strength	Limitation
Software AG	Comprehensive device connectivity (a specialized device management platform)	Loose augmented reality solutions integration in the platform, limited pre-built support for business KPIs
Hitachi	Rich & intuitive management console, various use cases	Limited wireless connectivity options, less pre-built apps, less strategic partners & resellers
GE Digital	Various pre-built apps for data analysis from industrial machines	Weaker monitoring & alerting functions, weaker support & training
Atos	Strong solution development for industrial customers, rich partner ecosystem (AWS, Azure), provide development, hosting, and integration services to Siemens MindSphere customers	Lacking pre-built solutions
Oracle	Rich pre-integrated apps, rich Oracle native features (Java Cloud Suite; ElasticSearch, Oracle Big Data Cloud, Oracle DB Cloud, Oracle NoSQL, Oracle Storage Cloud)	Limited industry-specific interfaces, limited strategic partners, limited augmented reality solutions
Siemens	Rich pre-built apps, growing community of 3rd party developers & partners, wide range of hardware devices for deployment	Weak set of KPIs at the MindSphere OS, weaker device management capabilities
Bosch	Strong industrial device controls, use both AWS cloud and Bosch IOT cloud, open source platform key components, strategic partnership with Eclipse Foundation and OSGi Alliance	Weak analytics, less compelling 3rd party apps & services
Schneider Electric	Pre-built apps extendibility to local requirements, growing network of partners & developers, rich, integrated, and stable industrial equipment (Schneider products)	Lacking multi-vendor device support
AWS	Wide range of database, analytics, & storage services	Less pre-built apps, small in-house professional service team
Cisco	Vast global telecom partnership to connect, manage, & monitor SIM-based IIOT devices, user-friendly control center	Disjointed UI between Cisco Jasper (SIM card based monitoring) and Cisco Kinetic (gateway management, edge processing, data control functions), limited support for industrial IOT use cases

At the more granular level, author of [3] divides IoT platform comparative analysis into nine function domains, which are Application Development, Device Management, Heterogeneity Management, Data Management, Statistical Analysis, Deployment Management, Monitoring Management, Visualization, and Research. The outcomes are summarized in the tables below (Tables 2, 3, 4, 5, 6, 7, 8, 9 and 10).

Table 2. IoT application development domain: actuator vetted assessments

Platform	Strength	Limitation
KAA	NoSQL DBs (Cassandra, Hadoop, MongoDB), open source	Lesser hardware modules supported
Carriots	Trigger-based apps, custom alarms, NoSQL DBs	Less user-friendly interface
Temboo	Choreos based apps: Yahoo weather, Amazon cloud, Ebay shopping, Flockr photo management, Facebook Graph API, Google Analytics, Twitter, Twilio, Paypal, Youtube, etc.	Unsuitable for resource intensive application

Table 3. IoT device management domain assessments

Platform	Strength	Limitation
SeeControl	Open API based push/pull architecture to support wide range of devices	Poor visualization
SensorCloud	Ability to manage massive sensor devices from Lord Microstain's	Open source devices are harder to manage
Etherios	Specialized clouds for devices & 3rd party software are provided, 30-day trial for 5 devices	Developers are restricted by selected devices
Xively	Easy to integrate devices; flexible API	Notification services are minimal
Ayla's IOT Cloud Fabric	Easy mobile application development	Unsuitable for small scale developers
thethings.io	Various connection protocols are able to connect varieties of devices	Lacking self-sustainance, dependent on 3rd party web services
Exosite	Easy system development	Lacking big data provisioning

Table 4. IoT heterogeneity management domain assessments

Platform	Strength	Limitation
Arrayent Connect TM	Flexible to use	Lagging at trigger-based services
Open remote	Open cloud service is provided	Too costly for developers

Table 5. IoT data management domain assessments

Platform	Strength	Limitation
Arkessa	Enterprise enabled design facet	Poor visualization
Axeda	Machine-to-machine based data management	Lacking self-sustainance, dependent on 3rd party web services
Oracle IoT Cloud	Sophisticated database support	Lacking open source devices connectivity
Nimbits	Easy to adopt for developers	Insufficient real-time query processing
ThingWorx	Easy to build data intensive app	Limited number of devices that can be attached

Table 6. IoT statistical analysis domain assessments

Platform	Strength	Limitation
InfoBright	Knowledge Grid architecture	Incomplete statistical services
Jasper Control Center	Rule based behaviour patterns enabled	Insufficient for automation services

Table 7. IoT deployment management domain assessments

Platform	Strength	Limitation
Echelon	Providing complete set of industrial-grade modules; microchips, protocols, management software	Lacking development scenario for beginners

Table 8. IoT monitoring management domain assessments

Platform	Strength	Limitation
AerCloud	Scalable machine-to-machine services	Not suitable for developers
ThingSpeak	Public cloud enablement with triggering facility	Less simultaneous number of devices connectivity

Table 9. IoT visualization domain assessments

Platform	Strength	Limitation
Plotly	Comprehensive visualization tools	Limited amount of storage
GroveStreams	Seamless event monitoring	Lacking statistical services

Table 10. IoT research domain assessments

Platform	Strength	Limitation
Microsoft Research Lab of Things	Suitable for home automation	Lacking IoT supported APIs
IBM IoT	Device identity (identity as a service)	Difficult for application prototyping

The above presented IoT platform comparative analyses imply the high importance of IoT platform assessment area, even if done only at the high level without delving into technical and management details. Hence, this paper's significance is justified since it formulates and delivers deeper and more detailed IoT platform assessment KPIs.

3 IoT Platform Assessment Enhancement Method and Outcomes

The eight dimensions of CREATE-IoT assessment standard [1] are comprised of constituents and each constituent has its own Key Performance Indicators (KPIs) or identifiers - with every KPI examines different elements of IoT platform - be it technical, management, or business-related element. The next table's left column presents these dimensions and constituents, while the existing current KPIs are omitted for brevity purpose.

The workable method in order to enhance the CREATE-IoT assessment standard [1] is direct IoT platform assessment, which consists of studying the IoT platform's technical architecture and business model. These would help formulate the new KPIs, which are currently missing from the CREATE-IoT assessment standard [1].

After studying IoT platform's technical architecture and business model in his IoT consultancy career journey, the author of this paper finally formulates 22 new IoT platform assessment KPIs, which are subsequently merged into the existing CREATE-IoT assessment standard [1] that originally consists of 198 KPIs. Each of them is listed on the right column next to the constituent on the left column where it is categorized under. The table below concludes this newly enhanced standard (Table 11).

Table 11. Integration of existing CREATE-IoT constituents and the newly formulated KPIs

Existing dimension & constituent	Newly added KPI
1. **Dimension:** Technology development	
Constituents:	
IoT devices and modules	1. *Options for IoT Device Additions* Description: The current industrial methods for device additions are as follows: • Plug-in based (JSON-based and MQTT-based) for external components i.e., device connection, service integration • Software Development Kits (SDKs) e.g., SDKs for Arduino, ESP, Raspberry PI, etc. • HTTP-based or CoAP-based device integrations In addition, simulation prior to deployment is recommended for safety measure. An example of IoT platform, which provides sophisticated device integration options is PTC Kepware [4]. It features the following: • Centre of device connectivity standards to simplify the management of device drivers and plug-ins • Telemetry configurations with modem, scheduling, etc. • Quick project deployment using automatic tag generation and device discovery • One-click mapping from industrial tags to properties on the IoT platform • Ability to push full projects from the IoT platform to a remote connectivity server • Configuration API for 3rd-party server management • Simulation options for testing prior to deployment • Data conditioning and compression, in order to minimize bandwidth and resource utilization • Machine-to-Machine (M2M) connectivity between homogeneous and heterogeneous systems • Consistent UI to manage device connectivity 2. *Availability and Readiness of Device Facing APIs* Description: Some abilities of device-facing Application Programming Interfaces (APIs) include the following: • Receive events from devices • Receive filtered queries • Send events to devices • Video stream load and retrieve files • Update device configuration • Upgrade firmware • Synchronize with edge processing An IoT platform that is a leader in this area is Software AG Cumulocity IoT [5], which delivers the following features: • Same APIs and same interface technology for all use cases • Various interfacing technologies i.e., HTTP, HTTPS, REST • New user interface functionality can be developed using plug-in

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
	3. *Supported Varieties of Device Types* Description: The varieties of device types depend on the needs of the use cases. Nevertheless, common device types are RFID, acoustic, automotive, navigation, pressure, force and level, temperature, humidity, proximity, etc. PTC [4] and Software AG Cumulocity IoT [5] are the shared leader of varieties of device types as each of them supports more than 150 types of device. There are also generic sensor devices such as Raspberry Pi, Cinterion boards, and Tinkerforge sensors 4. *Long Term Cost Efficiency of IoT Platform's Compatible Devices* Description: In order for IoT platforms operations to sustain for long period, they need to be economical and legally compliant to local regulations, thus locally manufactured IoT devices should be prioritized, unless the required function can only be fulfilled by imported devices. This is due to local devices being built usually with local compliance in mind 5. *Device Security* Description: The activities for securing IoT devices may include the following: • Minimizing exposure of ports or services to the Internet • Individual device registration to anticipate emergency disconnection measure in case the compromised device needs to be isolated • Changing the device's default username and password • Ensuring devices have enough memory for firmware upgrades and to encrypt communications • Encrypting the device's database/storage • Encrypting data transmission from and to the device; use only secure protocols Special for devices exposed to the Internet, they better support the following key cryptographic capabilities: • Data encryption with minimum 128-bit AES symmetric-key encryption algorithm • Digital signature with minimum 128-bit symmetric-key signature algorithm • TCP connection with minimum encryption layer using TLS version 1.2 or DTLS version 1.2 encryption layer for datagram-based communication paths • Unique key identification for every device that is stored securely (encrypted) on the device; this key should be updateable regularly over the device's link interface, or immediately if an intrusion towards the platform is detected • The device's firmware should be updateable Also, physical manipulations of IoT devices could be prevented by the below precautions: • Equip microcontrollers/microprocessors/auxiliary hardware with secure storage and cryptographic keys such as Trusted Platform Module (TPM) integration • Equip TPM with a secure boot loader and software loading • Gate the surrounding of the IoT devices with security sensors e.g., CCTV with motion recognition to detect trespassers. Further mitigation may involve "digital self-destruction" when the device is compromised

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
IoT platforms	6. *Platform Security at the Device Border* Description: IoT platform security at the device border can be built by the following actions: • Device registration and whitelisting. Other whitelisting methods may also be used i.e., network-based, serial number-based, or SIM-based • Device spoofing prevention • If possible and necessary, map every device to single user for better track of usage • Encrypt the connection from the device to the platform's back-end
IoT system monitoring	
IoT architecture	7. *Size of Data Storage* Description: The data storage should be able to accommodate massive data economically (may be achieved through data summarization method), it should also be scalable without downtime (may be achieved by high availability architecture or redundant server), have long data retention period (years or even infinite), and have adjustable computing power subject to the load An IoT platform that provides industry leading data storage is Microsoft Azure IoT [6] – with their separate databases for warm and cold data, which are mentioned below: • Azure Cosmos DB for warm storage: holds recent data (within seconds since ingestion) that needs to be accessed with low latency • Azure Blob Storage for cold storage: holds historical data that may tolerate higher latency • Azure Time Series Insights (TSI): an analytics, storage and visualization service for time series data, providing capabilities such as SQL-like filtering and aggregation • Azure SQL DB: max. capacity: 4 TB, throughput limit: max 4000 DTUs/eDTUs per database/Elastic Pool • Azure Data Lake: unlimited distributed data store that can persist large amounts of relational and nonrelational data without transformation or schema definition
IoT system functional design	8. *Service Redundancy or High Availability (HA) Mechanism* Description: Service redundancy provides the following capabilities: • Service fail-over and cross-region fail-over • Scaling the solution on multiple sites • Multi-site with roaming (device is homed in one of the sites, but may connect to the closest datacenter location based on proximity estimation; the collected information is routed to the home site of the device) • Multisite-multihome (device may roam across sites, and captured data is stored across the various sites that the device connects to, and can be collected and consolidated as required) • Isolation of service interruption; upgrades do not affect service (separated by broker that provides buffer; multiple brokers exchange data)

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
IoT verification, validation, testing and certification	9. *IoT Platform Audit* Description: The IoT platform should be audited continuously to guarantee performance and ensure SLAs are met; monitoring tools should be deployed to supervise the following statuses in the IoT platform: • Whether devices or systems are in erroneous state • Whether devices or systems are correctly configured • Whether devices or systems are generating accurate data • Whether the IoT platform is achieving the expectations of both business and end customers according to Service Level Agreements (SLAs) • Security-wise, Vulnerability Analysis (VA) may be conducted every 4 or 6 months, while penetration testing may be done once a year. Code check should be done in every application deployment. And logs monitoring should be done daily • IoT specific AI-driven vulnerability scanner tailored for Smart House and IoT devices could also be utilized, such as the one offered by Cybersecurity Help [7] Both Software AG Cumulocity IoT [5] and Microsoft Azure IoT [6] provide visual tool for auditing/monitoring. Azure IoT has Azure Operations Management Suite (OMS), Application Map, and App Insights for operations monitoring, logging, and troubleshooting, while Software AG Cumulocity IoT gives an auditing interface to capture security-relevant events and enable applications and agents to write audit logs, which are persistently stored and cannot be externally modified after being written. Audit records related to login and device control operations are also included
2. **Dimension:** Technology deployment and infrastructure	
Constituents:	
Use of open technologies devices and platforms	
Use of supported standards	
Capacity to solve interoperability and connectivity issues	
Scalability	10. *Reporting Capability and Expandability* Description: Report generation should not hamper the IoT platform. The IoT platform should be capable to store all produced reports for long period or even for infinite duration. In order to achieve this, report generation may be done by a dedicated data analytics cluster. However, each reporting duration may be determined by the complexity of data analytics models 11. *Tenants' Share of Events* Description: In a multi-tenant IoT platform environment, where there are multiple verticals (fields of IoT implementation) handled by different offices in the same IoT platform provider, there may be a need to share data and events among tenants, for examples: sharing of device definitions, sharing of sensor data, etc.

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
Efficiency in the maintenance, deployment and life-cycle of services and software running	12. *Affordability of Service Performance* Description: The cost of service performance may be related to the time duration to execute a transaction flow or the fee for every unit of ingested transaction per unit time, or other possible metric Software AG Cumulocity IoT [5] has structured costing for the amount of ingested data into the platform - For every additional request (inbound data), it costs €3 per 100,000 API and this is billed monthly Performance cost could revolve around the following factors: • Number of users • Data ingested over time or transactions per second (TPS) • Number of rules • Complexity of rules • Number of service APIs A transaction is defined as a complete flow through the IoT platform; from Event message to the Message Bus, on to the Event Consumer Service, getting information from the Device admin service, sending information to the Scene Evaluation Engine, and then sending to the Device Interaction Engine to send the message to perform a resultant action. Since a transaction is event based, the number of rules is not linear to TPS. In order to cater to growing TPS, a capable and scalable message broker must be utilized. A scalable and affordable public cloud infrastructure is also desired for an economical yet significant performance improvement An example of a transaction is the one described by GE Predix Platform's [8] wind forecasting application. For its deployment of four wind farms, the application ingests data from edge/devices, runs analytics on the data, and then sends the analytics results to the edge. All this flow is accomplished in 18 s It is a general practice to reduce operation cost by migrating to Docker on AWS. Computing power is expandable via AWS settings. An enterprise-grade message broker such as RabbitMQ may also be deployed to cater more connections compared to entry level brokers like ActiveMQ. For even larger scaling, an MQTT-based message broker could be used 13. *Affordability of Data Storage* Description: The cost of data storage should be economical for future scalability and storage scaling should not require downtime (may be achieved by redundancy or HA architecture) - in order to preserve data service. Furthermore, data storage cost could be reduced by data summarization Moreover, the cost of data storage would be more affordable and scalable when data storage is outsourced to public cloud, such as AWS. Even so, there may be a need to make use of private data centre in case sensitive data needs to be stored locally, or when local data retention is enforced by the local authorities. On the downside, storing data in private data centre usually costs more than utilizing public cloud storage; this is due to development cost and infrastructure cost (electricity, premise building and maintenance, security cost, etc.)

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
	Both Software AG Cumulocity IoT [5] and Microsoft Azure IoT [6] offer structured data storage costing based on utilized storage and ingested request count. A detailed information on bundling of storage limit and request count for Standard Tenant packages is given by Software AG Cumulocity IoT [5] as follows: • Standard Tenant Bundle Pricing I: €500/month (€5/device/month), 12 months term, business support included, max. 100 devices supported, 2 millions inbound data transfers per month, 10 GB storage • Standard Tenant Bundle Pricing II: €1,500/month (€3/device/month), 12 months term, business support included, max. 500 devices supported, 10 millions inbound data transfers per month, 50 GB storage • Standard Tenant Bundle Pricing III: €2,500/month (€2.5/device/month), 12 months term, business support included, max. 1,000 devices supported, 20 millions inbound data transfers per month, 100 GB storage • Standard Tenant Bundle Pricing IV: €3,500/month (€0.35/device/month), 12 months term, business support included, max. 10,000 devices supported, 5 millions inbound data transfers per month, 10 GB storage • Additional storage costs €1 for every 100 MB per month
Integration with the existing and new infrastructure	
3. **Dimension:** Ecosystem strategy and engagement	
Constituents:	
Ecosystem awareness	
Stakeholders' engagement	
External partnerships and collaboration	
Public and government engagement	
4. **Dimension:** Ecosystem openness and external collaboration	
Constituents:	
Value chain openness	
Inclusiveness and participation for third parties	14. *Value-Adding Data from External Sources or 3rd Parties* Description: Freely available external data sources may be integrated to trigger specific actions, for example: external weather forecast data that triggers watering sensors and actuators in a smart greenhouse IoT implementation An established IoT platform that fulfils external data sources integration is IBM IoT [9], which integrates weather, maps, and social media data Typically, external data can be queried or integrated easily via APIs

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
Openness of business models	
Open source strategy	
5. **Dimension:** Marketplace and business impacts	
Constituents:	
Business models	
Market readiness and monetization mechanisms	15. *Sale Package* Description: IoT service sale bundling is subject to the state of supply and demand for the target market. An infant IoT market may start by bundling on cellular data package usage, which incorporates IoT platform service in its offer. While an IoT market in stable growth may offer independent IoT platform service package, this independent offer is related to the provided vertical solutions e.g., smart house, smart parking, etc. Sale package could also be designed based on the following factors: 1. Number of devices 2. Number of users 3. Subscription term 4. Data ingestion rate 5. Data storage 6. Services offered 7. Platform-to-platform (P2P) offered 8. Selections of device's link interfaces, whether it is Wi-Fi, NB-IoT, 5G, SigFox, ZigBee, or others 9. Data analytics methods 10. User customization options
Business benefits	
Market competitiveness	
Legal issues	
Privacy, security, trust and ethical issues	16. *Data Expiry* Description: Data expiry is also known as data aging or data deletion after certain period – usually subject to SLA, for example: GE Predix [8] defines a contract that mentions the responsibilities of parties in the life cycle of sensitive data, which includes data retention and data deletion; the longer the data retention the safer it is for data aging practice There is also a useful temporary data retention feature at the edge device called inbox-mode, which stores data and command for a device when it loses connection to the edge hub – and when the device regains its online connection, it will receive the cached data and command from the edge hub 17. *Tenants' Regulated Data Sharing* Description: This is the ability to conduct and regulate data sharing securely among tenants by enabling event subscription. It is useful to exchange data among different verticals of IoT implementation. Besides events, tenants may also share device definitions in case the same devices would be deployed by different tenant/s

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
	18. *Technically and Legally Compliant IoT Platform* Description: A technically and legally compliant IoT platform should comply to the following: • Secure Software Development Life Cycle (SDLC) • IT security guidelines e.g., OWASP, WASC, ISO 27001 • Privacy and data protection legislation by the local authority • Vertical, application layer, or software architecture standard: Domain Driven Design (DDD) • Architecture and documentation standard: TOGAF • Process-related activity standard: ISO 9001 Furthermore, support from the local government may also encourage the growth and compliance of IoT platform, for example: Sri Lankan and Malaysian government [10] give tax compensation/exemption for IoT-related infrastructure development An example of compliant practices is done by IBM IoT [9], which includes: • Certifications: ISO 27001, ISO 27017, ISO 27018, ISO 9001, ISO 22301, ISO 31000, SOC 1, SOC 2 and SOC 3, PCI, HITRUST, FedRAMP, IRAP (Australia), ISO 14001, ISO 50001, OHSAS 1800 • Global regulations: EU Model Clauses, FERPA, HIPAA, My Number Act (Japan), United States International Traffic in Arms Regulations (ITAR), Cloud Computing Compliance Controls Catalog (C5) (Germany) • Alignments and Frameworks: Criminal Justice Information Systems (CJIS), The Cloud Security Alliance CSA, EU-US Privacy Shield, Federal Financial Institutions Examination Council (FFIEC), The Center for Financial Industry Information Systems (FISC), The Federal Information Security Management Act of 2002 (FISMA)
Experience readiness level	19. *Rule Activity Management (Programmable Rule)* Description: An established IoT platform should be able to provide an interface to program IoT scenarios i.e., Stateless processors and static rules are preferable if analysis rules do not change and do not refer to dynamic external data. Furthermore, stateless processors and static rules are suitable when the following conditions exist: • Input data records are serialized in JSON format • There is only small number of rules • Data records can be analyzed one at a time i.e., there is no need to aggregate data over multiple data points (e.g., averaging) or data streams (e.g., merging data from multiple devices) On the other approach, stateful processors and dynamic rules are more appropriate for scenarios, where flexibility is desired to support variable load, frequent changes to stream processing logic, and mutable external reference data. In details, they are suitable for the following conditions: • Input data records demand advanced analysis, such as time windows, streams aggregation, or joining with external data sources - which is not possible with the stateless architecture • The processing logic has rules or logic units, which might grow significantly along the way • Input telemetry data is serialized in a binary format like Avro Moreover, safety measures for action rule can be implemented as follows: • Simulate the rule before it is deployed • Utilize rule versioning system, in order to provide rollback capability

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
	• Add a feature to control additional information points within a scene or action rule • Add scheduling feature to rules i.e., rule actions may depend on time of the day e.g., a rule may state that when Event A occurs and time is earlier than 10am, then execute Action X, or else do Action Y • Add nested rules feature to anticipate complex scenario • Embed safety-related Artificial Intelligence (AI) capability at edge processing An example of IoT platform that provides programmable rule is SAP Leonardo IoT [11], it utilizes insight of device data to trigger appropriate actions in the business systems. It also makes use of the IoT capabilities of the SAP Cloud Platform to offer more varieties of services 20. *Self Navigation for Reporting and Data Analytics* Description: Ideally, IoT platform users should be able to maneuver through data analytics and reporting features independently without the assistance of dedicated data scientists. User-friendliness in data analytics is a sign of readiness of an IoT platform; the more sophisticated the platform, the simpler the feature navigation Data analytics server or cluster may be made accessible via a set of APIs e.g., Apache Solar indexes or Power BI. In case each vertical's data is stored in separate tables in order to enforce privacy, on the downside, this might make it harder to conduct cross-vertical analytics when it needs to merge data from different verticals Based on Forrester 2018 IoT platforms comparative analysis report [2], Microsoft's advanced analytics that are based on open source technology makes them the best in analytics category [6]. Specifically, Microsoft Azure IoT's analytics capability includes HDInsight. Power BI, Apache Spark 21. *Comprehensive Reporting and Data Analytics* Description: At minimum, any IoT platform should fulfil common purposes of data analytics, which include the following: • Pattern recognition • Anomaly detection • Frequency finding • Parameter values over time distribution (behavior analysis) • Mapping or heat mapping • Event prediction • Behavior or action detection • Causality and correlation analysis In an IoT platform vertical, comprehensive reporting and analytics should be able to fulfil the objectives of the deployed use cases – within the reasonable time - even when under maximum load capacity In Feb 2017, Google conducted research about the average mobile web page load times across different industries [12] and discovered that the average load time duration was 8.66 s. They further recommended that a reasonable duration should be below 3 s. Therefore, if data analytics process is added to the duration, then analytics report generation within this duration or a little above it would be deemed acceptable

(*continued*)

Table 11. (*continued*)

Existing dimension & constituent	Newly added KPI
	In general, all IoT platforms are capable to do data analytics and reporting, however IBM IoT [9] and C3IoT [13] are considered leaders in this area with their varieties of pre-built applications and use cases. Specifically, for C3IoT, their analytics features provide the following: • C3 Data Science service: a complete AI/ML capabilities to generate an accurate prediction, and offers configurable visualization methods, including time-series, tables, charts, scatter plots, etc. • C3 Data Science service: a visual tool to build analytics process pipeline
Holistic innovation	
6. **Dimension:** Societal and economic impacts	
Constituents:	
Indirect revenue generation	
Employment macro-impact	
User worktime/life impact	
Targeted social groups	
7. **Dimension:** Policy and governance impacts	
Constituents:	
European IoT ecosystem promotion and competitiveness safeguard	
IoT standards promotion	
Trusted, safe, secure IoT environment promotion	22. *Multi-tenant IoT Platform* Description: In common practice, the IoT's hierarchical platform would allow the top boss or the super admin of the company to access all IoT verticals owned by the company, while a branch office head or branch manager would only be allowed to access their own vertical. This practice would enforce data privacy and legal compliance towards the SLAs and the local governmental regulations
Impact on SMEs, start-ups and young entrepreneurs	
8. **Dimension:** Community support and stakeholders' inclusion	
Constituents:	
Developers' community accessibility	
Education availability	
Accessibility levels	
Community engagement	

4 Conclusion

The existing CREATE-IoT IoT platform assessment standard [1] has been successfully enriched with sizeable 22 new essential KPIs. In other words, the overall enhancement is 11.11% from the original number of KPIs (198). This is considered significant as all additions are unique and necessary; they would significantly increase the quality of IoT platform assessment outcomes and may be used by IoT platforms all over the world. Nonetheless, this enhanced standard would also drive new IoT deployments worldwide as it gives confidence of the readiness state of the assessed IoT platform – as well as its legal compliance.

More IoT deployments mean more jobs would be created, thus it is beneficial for the global economy. This would also connect and modernize different nations in sophisticated ways through sharing permissible IoT events and data, which are fundamental for acceleration of national infrastructure automation purpose.

References

1. Micheletti, G., et al.: Common methodology and KPIs for design, testing and validation. In: Cross Fertilisation Through Alignment, Synchronisation and Exchanges for IoT, pp. 1–49 (2017)
2. Miller, P., Pelino, M.: Industrial IoT software platforms, Q3 2018: the 15 providers that matter most and how they stack up. In: The Forrester Wave (2018)
3. Ray, P.P.: A survey of IoT cloud platforms. Fut. Comput. Inform. J. **1**(1–2), 35–46 (2016)
4. PTC IoT (2020). https://www.kepware.com/en-us/industries/internet-of-things/2020/11/6. Accessed 11 Jun 2020
5. Software AG Cumulocity IoT (2020). https://www.softwareag.com/en_corporate/platform/iot.html/2020/11/6. Accessed 11 Jun 2020
6. Azure IoT (2020). https://azure.microsoft.com/en-us/overview/iot/2020/11/6. Accessed 11 Jun 2020
7. SaaS Vulnerability Scanner (2020). https://www.cybersecurity-help.cz/security-services/saas-vulnerability-scanner.html/2020/11/6. Accessed 11 Jun 2020
8. GE Predix (2020). https://www.ge.com/digital/iiot-platform/2020/11/6. Accessed 11 Jun 2020
9. IBM IoT (2020). https://www.ibm.com/cloud/internet-of-things/2020/11/7. Accessed 11 Jul 2020
10. Halim, A.H.A., et al.: National Internet of Things (IoT) Strategic Roadmap. MIMOS Berhad (2014). https://www.mestecc.gov.my/web/wp-content/uploads/2017/02/IoT-Strategic-Roadmap-1.pdf
11. SAP Leonardo IoT (2020). https://help.sap.com/viewer/product/SAP_Leonardo_IoT/1904b/en-US/2020/11/11. Accessed 11 Nov 2020
12. Google Research. https://www.machmetrics.com/speed-blog/average-page-load-times-websites-2018/
13. C3IoT (2020). https://www.welcome.ai/tech/data-resources-management/c3-iot-c3-iot-platform/2020/11/11. Accessed 11 Nov 2020