

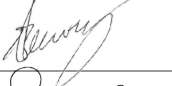



## SCOPE OF WORKS

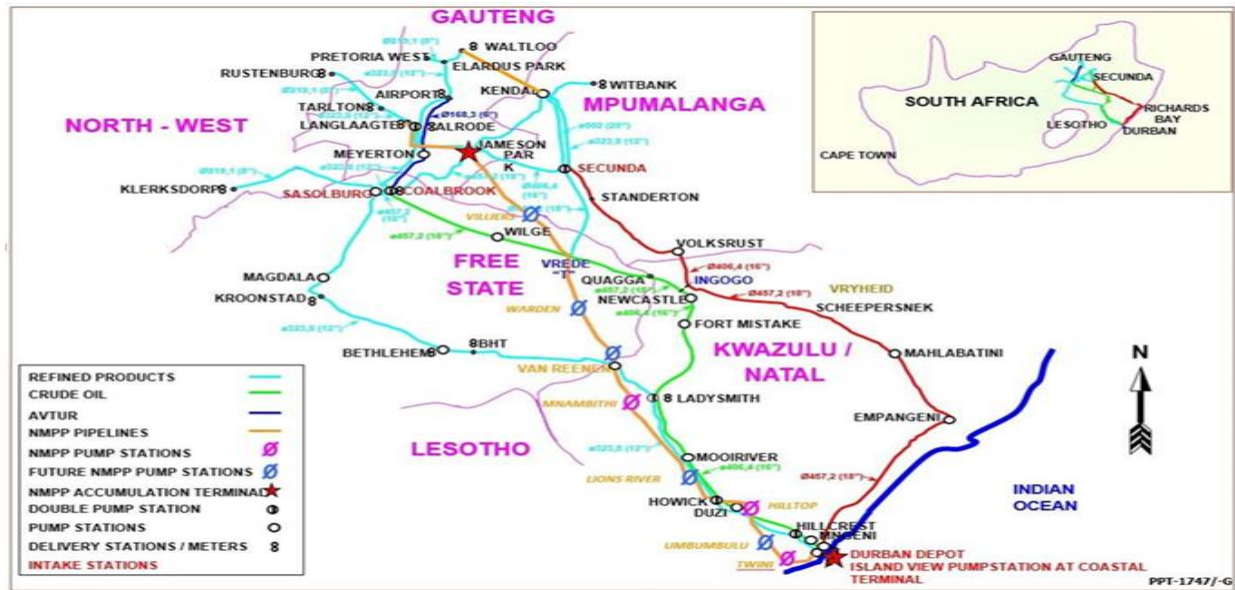
### IoT INTRUSION DETECTION SERVICES FOR TRANSNET PIPELINES

	Name	Signature	Date
<b>Prepared by</b>	Yanga Manana (Security Systems Specialist)		September 2022
<b>Reviewed by</b>	Nathi Ndlovu (Project Manager)		September 2022
<b>Supported by</b>	Richard Sewraj (Chief Security and Forensics Officer)		September 2022
<b>Approved by</b>	Razien Samuels (Head ICT)		September 2022

Glossary of Abbreviations and Acronyms	
<b>Transnet Pipelines</b>	TPL
<b>Internet of Things</b>	IoT
<b>Block Valve</b>	BV
<b>National Operation Centre</b>	NOC
<b>Service Provider</b>	SP
<b>National Key Point</b>	NKP

## A. BACKGROUND

Transnet Pipelines (TPL) is the largest multi-product operator in Southern Africa, transporting hydrocarbons and methane-rich gas through a network of 3 800 KM's of petroleum and gas pipeline infrastructure of which 3 116 KM's is currently operational. The pipeline network traverses five different provinces in South Africa (KwaZulu-Natal, Free State, Gauteng, North West and Mpumalanga) ensuring security of petroleum supply to the inland market and methane rich gas to Kwa-Zulu Natal.



Transnet Pipeline National Network

The pipelines are buried underground with above ground supporting equipment's (e.g. test points, rectifiers, concrete makers and block valves). Block valve (BV) chambers reside on the pipelines servitudes area at approximately 15 km's to each other depending on the topography. These BVs allow sections of the pipeline to be isolated during leaks, testing for leaks, and other maintenance and reactive maintenance activities. BV chambers are usually 3 meters in length, 2 meters in width and 2.5 meters in depth on average. There are equipment's contained inside the BV's which are critical for the pipelines operation that are maintained on an occasional and planned basis.

There are two types of BV chambers: one type is secured with steel, welded around the chamber with padlocks on the chamber steel doors and the other type has concrete slabs covering the BV chamber surface.

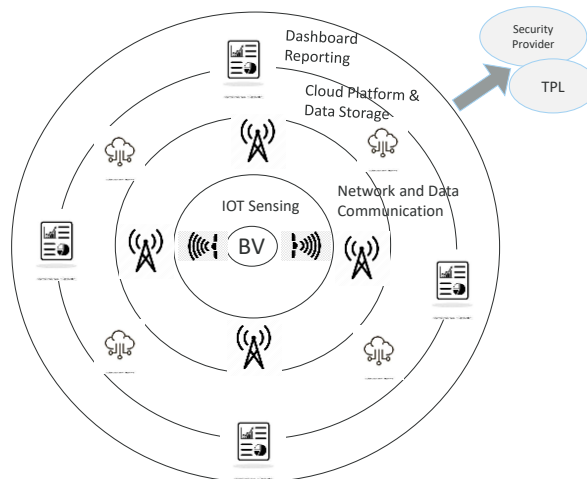
The BV's are classified as an Essential Infrastructure (EI) or Critical Infrastructure (CI). "According to the CI Protection Act 8 of 2019, measures shall be put in place for the protection, safeguarding and resilience of the CI".

The following challenges currently exist at the BV's that need to be considered within the scope of work when designing, implementing or supporting the environment:

- Many of TPL BV's are located in remote areas without electrical or communication infrastructure present. (Refer to **Annexure A** for block valves location areas).
- The access route to these BV's is typically bad such that in most cases, BV is accessible by 4-wheel drive vehicle only.
- Some of the BV's are accessible through the farmer's land, which requires the landowner's permission for access. TPL to facilitate access requirements.
- No structures exist around the BV's area which can be used to aid with additional components installation.
- Any equipment that is erected around the BV's area will become a target for theft.
- The communication network coverage to some areas is poor, other areas have no network coverage at all.
- BV's are not all one dimensional in size, and are covered in either steel or concrete lids. (Refer to **Annexure B** for images of the typical two types of BVs').

## B. SCOPE OF WORKS

The Service Provider is required to deliver an outsource Internet of Things (IoT) service that detects and reports on intrusions at the 400 TPL Block valves in real time (24/7/365) for a contracted period of 3 years. This will include the design, implementation and maintenance of an end to end solution that consists of sensors, edge devices, networks, applications, databases, cloud platform & data storage with functionality to link to external parties, reporting dashboard and ability to communicate via means such as SMS, emails and instant messaging app.



The solution rollout will cover 2 distinct phases;

1. **SOLUTION CONFIRMATION** - The installation of the IoT intrusion detection solution on 20 block valves with an objective to establish solution effectiveness. Decision on solution go / no go will be made at this point.

2. It is the condition of this contract that the continuation of the Project Roll Out Phase is dependent on the successful establishment of the solution effectiveness. In the event the solution provided is not effective to Transnet's satisfaction and intended objectives that will amount to a material breach and Transnet reserves the right to Terminate the contract without prejudice in accordance with the Termination Clause as contained in the Master Agreement.
3. **PROJECT ROLLOUT** - Following the successful validation of the solution, the objective of this phase is to rollout the solution to cover an additional 380 block valves.
4. In addition, 20 IoT intrusion detection movable devices to be deployed as and when required on the pipeline network.

#### **FUNCTIONALITY OF SOLUTION**

5. The IoT device at the BV's must be positioned such that it is capable of instantaneous detecting any movement, vibration, tilting or opening of the concrete lids.
6. Alerts of intrusion must communicate within 15 seconds i.e. Notification / alert via SMS, email and instant messaging app, to the TPL designated team.
7. Alerts of intrusion must contain relevant information including BV name, co-ordinates and timestamp. GPS co-ordinates displayed must have the functionality to re-direct to map.
8. The IoT device shall be mounted internally or externally of the BV.
9. Internal installations must be certified for use in hazardous area i.e. classification code for Zone 1 (Exd or Ede).
10. The IoT devices must be weather proof rated (i.e. outdoor device). IP rating of IP67 or higher.
11. The IoT devices must be secured in a tamper proof enclosure.
12. The solution must be proven with a successful track record to function in an industrial environment with capabilities to operate in remote areas, urban or rural.
13. The IoT devices must confirm connectivity in 30 minutes intervals, via a heartbeat or equivalent method. In cases of no heartbeats or errors occurring, devices must issue another heartbeat in 1 minute and after 10 attempts (1 minute apart), an alert notification must be sent detailing no response from device. Other device error alerts to be addressed similarly.
14. The battery life of the IoT devices should be at least two years and should be optimised for the transmission of small amounts of data.

15. External charge mechanisms like solar panel and line power to power up IoT devices next to the BV's will not be considered.
16. The solution should also allow for two-way communication enabling over-the-air (OTA) firmware updates and remote debugging.
17. Installed IoT devices need to be able to communicate with more than one network infrastructure/facility such that redundancy is created to ensure maximum uptime.
18. The network must have acceptable range and coverage for all BVs.
19. IoT solutions and technologies must be proven and future-proofed and offered by financially sound telecommunication companies and Original Equipment Manufacturers (OEM's) in South Africa. Key technology roadmaps should be included in the proposal.
20. The system must be configurable to send notifications to selected user groups.
21. The end-to-end IoT solution must be designed, implemented and maintained to prevent cyber-attacks, loss of data, signal jammers and any other risks in its deployment.
22. All TPL data must be encrypted i.e. data stored on the Service Provider's (SP's) platform as well as data in motion.
23. The SP's data platform must prevent unauthorised data access and ensure sensitive Transnet data is secured.
24. A cloud platform is required for the storing of data, data engineering, application/dashboard and initiation of alerts and notifications to TPL.
25. The cloud platform must allow for the storage, authorised access and retrieval of historical data for the duration of this contract.
26. The cloud platform must "push" data to the Transnet Cloud or to Transnet service provider's platforms.
27. A web-based Application/Dashboard must illustrate all of the installed BV's in a map view with their applicable details and drill down functionalities. Alerts should be reflected on this application and sections to acknowledge and indicate closure of alerts. Detailed requirements include:
  - a. **Application/Dashboard (1)**
    - A design and implementation of a dashboard facility to illustrate and report.

- Display a graphical view of a map with the pipeline routes and BVs with installed devices.
- Illustrate device identification and location on the dashboard.
- Signal alarm status (e.g. Active/ Inactive).
- Report alarm classification (e.g. disturbance of device, vibration of structure, tilting of BV cover).
- Unprotected block valves.
- Handling of alarms (e.g. acknowledge, action, park, close).
- Provide message/alarm timestamp, location and pipeline name BV resides on.
- Authorised access to dashboard and/or selective functionality.
- Illustrate data connectivity status (e.g. metrics such as signal strength).
- Provide feature to extract data of present and historical events for analysis patterns for duration of contract.
- Dashboard must have the functionality to be updated, changed and expanded.

**b. Application/Dashboard (2)**

- A design and implementation of a dashboard facility to illustrate and report.
- Battery status of all devices.
- Network and IoT device status.
- Notification of supporting infrastructure damages or out of service components reliant by the network.
- Periodic signal/heart beat performance for installed devices.
- Alerts of missed periodic/ heart beats, low battery on devices (80% used Threshold) and alerts of system errors).
- List of all faults (Resolved/Pending/Outstanding).
- Ability to add and remove data fields from dashboard reports.

**SERVICE PROVIDER'S RESPONSIBILITIES SHALL INCLUDE THE FOLLOWING FUNCTIONS INTER ALIA:**

28. Provisioning of an end-to-end IoT solution to detect and report on intrusions in real time.
29. Positioning and the securing of devices on / in/ around the BV to ensure the detection of intrusion e.g. movement / vibration/ tilting/ opening.
30. Log faults and inform TPL of any devices/network/system errors timeously.
31. Device installation metadata creations: Naming convention (Naming method to specify BV number, pipeline name and sensor number).
32. Creation of the test plan for the installation of the IoT devices at the BVs including (e.g. signal strength test, alarm tests) for TPL's approval.

33. Replacement of deployed equipment in the event of theft or vandalism.
34. SP must carry sufficient stock on hand which have been configured and tested ready for installation.
35. SP must pro-actively monitor the IoT environment and inform TPL of any faults.
36. Maintenance and support of the IoT environment. (E.g. Maintenance of software patches and updates).
37. A detailed maintenance plan must be provided to TPL detailing the scheduled maintenance over the contract period.
38. Asset and spares management:
  - a. Register of Assets (Serial Numbers, Warranty status etc.)
  - b. Device decommissioning at the end of the lease period.
39. The SP must provide a ticketing system. The ticketing system must allow for logging and tracking of faults.
40. Advise TPL of emerging risks in the IoT environment and corrective measures.
41. Bi-annual site visits to selected BV's for redundancy testing as well as on site quality assurance.
42. Ensure that change control procedures are adhered to, for any changes including devices, systems, designs and access authorisation.
43. Provide TPL with a network solution that applies technology such as IoT network, NB-IoT, LTE, 3G,4G,5G, satellite etc, supported by a comparative assessments and recommendation for a suitable network mix.
44. SP is requested to price for each of the proposed networks.
45. Provision of periodic testing of the signal strength in order to ensure adequate signal and coverage during the lifetime of the contract and provide TPL with the assurance.
46. Signal strength baseline must be submitted for TPL approvals.
47. To ensure an end-to-end, real-time IoT solution, the SP must have a back-end integration to sub-contractor's application e.g. network service provider/s.
48. Ensure any network limitations or faults are reported to TPL.

49. Notification of supporting infrastructure damages or out of service components relied on by the network/s.
50. Ensure all deployed equipment installed on BV's and supporting infrastructure such as towers are maintained.
51. Subscriptions, sub-contractors, licenses, intellectual property (IP) and SLA's held by the SP must be disclosed to TPL on proposal and updated throughout the duration of the contract.
52. The SP to exercise care at the BV's infrastructure during installation, maintenance of devices and decommissioning.
53. All TPL information residing on the SP's devices, network or cloud data centre systems or hosted environments shall be removed at the end of the contract period. Requested data should be handover over to TPL.
54. Attend monthly and/or weekly meetings as and when requested by TPL.
55. The SP to provide the following reporting:
  - c. Monthly SLA report detailing SLA measurements met and missed.
  - d. Device management reports detailing device health, network status, battery levels etc.
  - e. Results of the periodic signal strength testing.
  - f. Asset register illustrating all device information.
  - g. Adhoc reports as and when required.
  - h. Maintenance reports.
  - i. Trend analysis reports.

**ON ISSUE OF THE LETTER OF INTENT TO THE SUCCESSFUL BIDDER THE FOLLOWING MUST BE PROVIDED:**

56. TPL will provide the SP with the list of all BV GPS Coordinates. The SP will need to confirm coverage and signal strength by completing physical due diligence at each BV within a period of 30 days. If the primary means of communication as per the proposal is inadequate, then the secondary means of communication must be provided. A detail list of all BVs with the recommended network communications is required.
57. SP to submit a detailed design document of the end-to-end solution, with indication of possible points of failure and the migrations that are included in the design.
58. SP to provide safety files of all personnel that will be working at the BVs within 30 days. Any changes of personnel during the contract period will require amended safety files.
59. SP must have their own armed security personnel accompanying their technical teams during the installations/support of IoT device at the sites. It is suggested that two armed guards be allocated.



**SOLUTION CONFIRMATION:**

- 60. Test plan to be co-created with TPL against which testing will be conducted, considering the critical success factors to solution effectiveness.
- 61. The installation of the IoT intrusion detection solution on 20 block valves the objective of testing the end-to-end solution.
- 62. Manage rollout, monitor solution effectiveness and confirm results of tests and level of success, documented in the solution results documentation.
- 63. With TPL, the SP to review the critical success factors against the solution test and confirm go or no go for the project rollout.

**ROLLOUT OF PROJECT:**

- 64. Following the successful solution validation and confirmation of the project rollout, the objective of the rollout phase is to complete the implementation across the remaining 380 block valves.
- 65. Deliver the project rollout phase by applying the standard Project Management approach, detailing project owners, responsibilities, delivery plan, actions, timelines and approach to problem resolution and risk mitigation that will be undertaken during the execution of this phase.
- 66. Successfully complete the installation of sensors at 380 block valves with full functionality, including data transfer, cloud and dashboard operations within the approved time frame.

## SLA CRITERIA

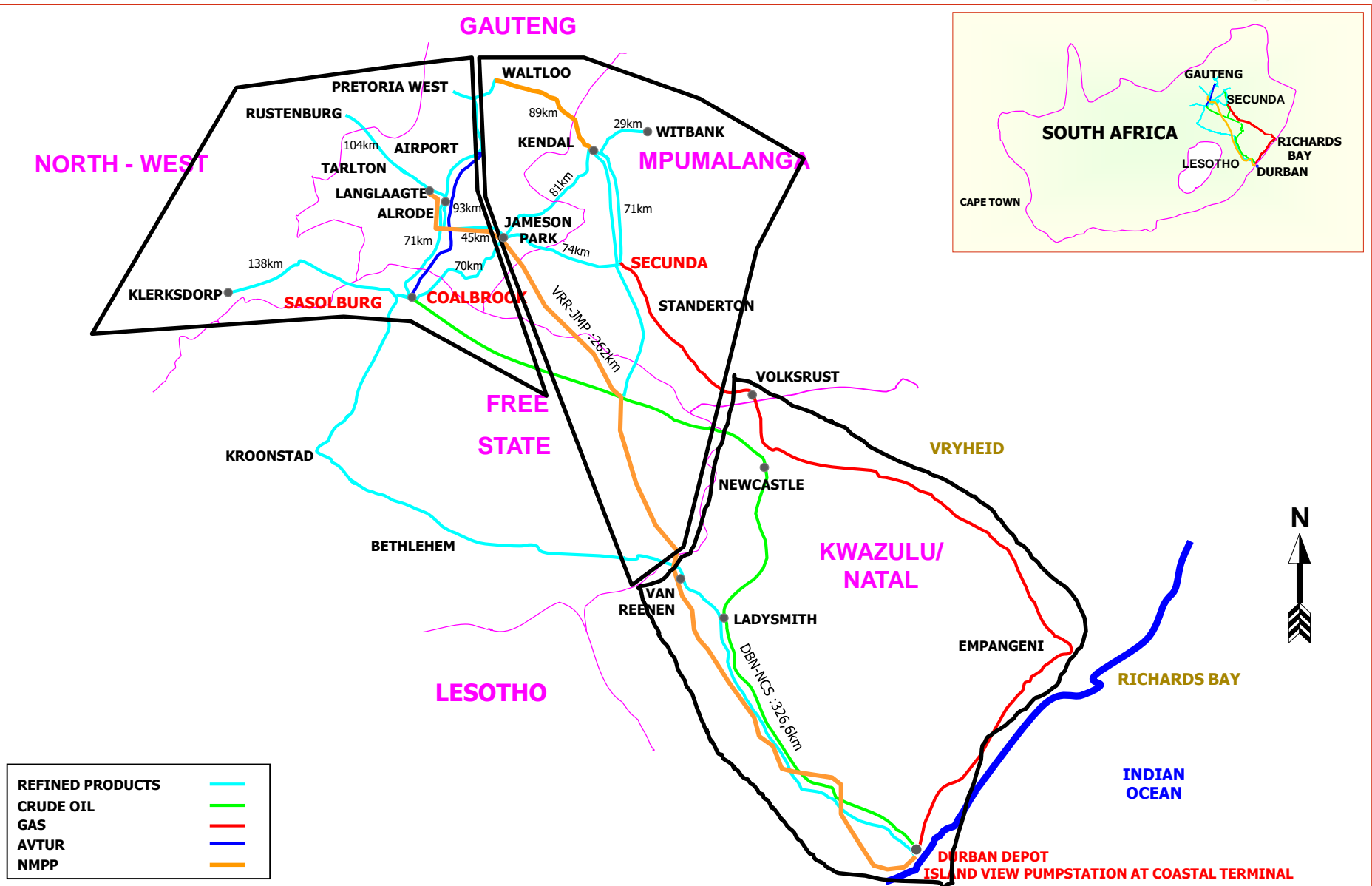
TPL Block Valve IOT Intrusion Detection Services - Service Level Agreement						
No	Area of Metric	Description of Metric	Service Level		Penalty	Comments
1	Block Valve fully protected ie 400 Block valves	Availability of all installed IOT devices transmitting data to Application/dashboard and messaging	Calculation: (number of BV multiplied by the number of hours in a month less sum of all unplanned downtime in the month) divided by number of BV multiplied by the number of hours in a month multiplied by 100.	99,5% of BVs are protected in a month	98,5%<=99,5%:5% of total monthly service fees; 97,5%<=98,5%:7% of total monthly service fees; <97,5%:10% of total monthly fees	Downtime includes devices, application, networks, platforms, messages, hardware, software and/ or any component that will cause the solution to be non-functional. (the SLA of 99,5% excludes devices damaged due to product theft incidents)
2	IOT Device/Edge faults (hardware)	Failure of device to sense relevant activity and communicate this data due to hardware faults	48 hours repair time	SLA of 48 hours must be achieved 100% of the time	48 hours >=72 hours : 2% of total monthly service fees; 72 hours >= 120 hours :3% of total monthly fees; >120 hours:4% of total monthly fees	Includes co-ordinating with TPL team, travel time and testing of device. This repair time also includes the replacement of devices due to vandalism/theft
3	Software related faults including IOT Device/Edge , application, configurations,dashboard, messaging faults (email/sms)	Failure of device to sense relevant activity and communicate this data. Fault can be resolved remotely	4 hours repair time	SLA of 4 hours must be achieved 100% of the time	4 hours >=12 hours : 2% of total monthly service fees; 12 hours >= 24 hours :3% of total monthly fees; >24 hours :5% of total monthly fees	
4	Periodic signal per BV notifications (pulse / heartbeat) in real time	Transmit a signal / pulse every 30 minutes. IOT devices is communicating via the network to the application/dashboard, in real time (no latency).	Failure rate of <=2% of pulses per device per month	100%	1% of total monthly service fees	Sensor/devices must confirm connectivity in 30 minutes intervals, via a heartbeat/pulse In cases of no heartbeats devices must issue another heartbeat in 1 minute and after 10 attempts (1 minute apart), an alert notification must be sent
5	Communication timelapse from Sensor detecting vibration/movement/tilting/opening of lid	Transfer time of 15 seconds for the data signal from IOT trigger to receipt in dashboard/alert messages	Transfer time of 15 second	100%	15 seonds >=5 minutes :0.5% of total monthly service fees; 5 minutes >= 15 minutes :1% of total monthly fees; >15minutes :2% of total monthly fees	
6	Notification of fault affecting security of the BV	defective devices, network faults etc	within 60 minutes	100%	3% of total monthly service fees	Service provider to monitor the environment end-to-end, log faults and send mail/sms notification with fault reference number to TPL; Note BV security will be comprised if one IOT device is faulty; no network or
7	False alarms	The frequency of false triggers / alarms due to device/system errors	Zero false alarms	100%	2% of total monthly service fees	A false alarm is defined as a system error that triggered an alarm.
8	Cyber Security	Zero security breaches	Zero security breaches	100%	2% of total monthly service fees	
9	Availability of spares (IOT devices)	5% of IOT's devices deployed. For example 100 deployed IOTs = 5 spare devices	5% of deployed devices	100%	1% of total monthly service fees	Spares must be available and kept at suitable locations
10	Maintenance	Completed maintenance to agreed maintenance plan	Planned maintenance = Completed maintenance	100%	1% of total monthly service fees	
11	Reporting	Accurate reports submitted by SP to TPL by the 5th of each month	Accurate report received by 5th of every month	100%	0,5% of total monthly service fees	

## IMPORTANT NOTES

- SP shall provide a detailed project execution/implementation plan.
- TPL recommended personnel must accompany all visits to any of TPL's sites.
- All work to be performed on TPL's infrastructure must be indicated prior for TPL's approval and must be supervised by TPL personnel.
- The SP will be liable for any damages to the current BV infrastructure caused during the installation, maintenance exercises.
- High level project plan and macro design document of the solution is required in the proposal submission.
- Resources allocated to the project must be highly skilled with experience in successfully completing similar projects.
- TPL reserves the right to amend the number of devices that are required to be deployed.
- All information pertaining to TPL and BV chambers are highly confidential as our infrastructure are classified as critical Infrastructure and a non-disclosure agreement will have to be signed.
- SP must bill TPL accordingly to the number of protected block valves in a given month (i.e all IoT devices on BVs' functional).
- At the end of the contract, TPL reserves the right to purchase devices located at BVs.

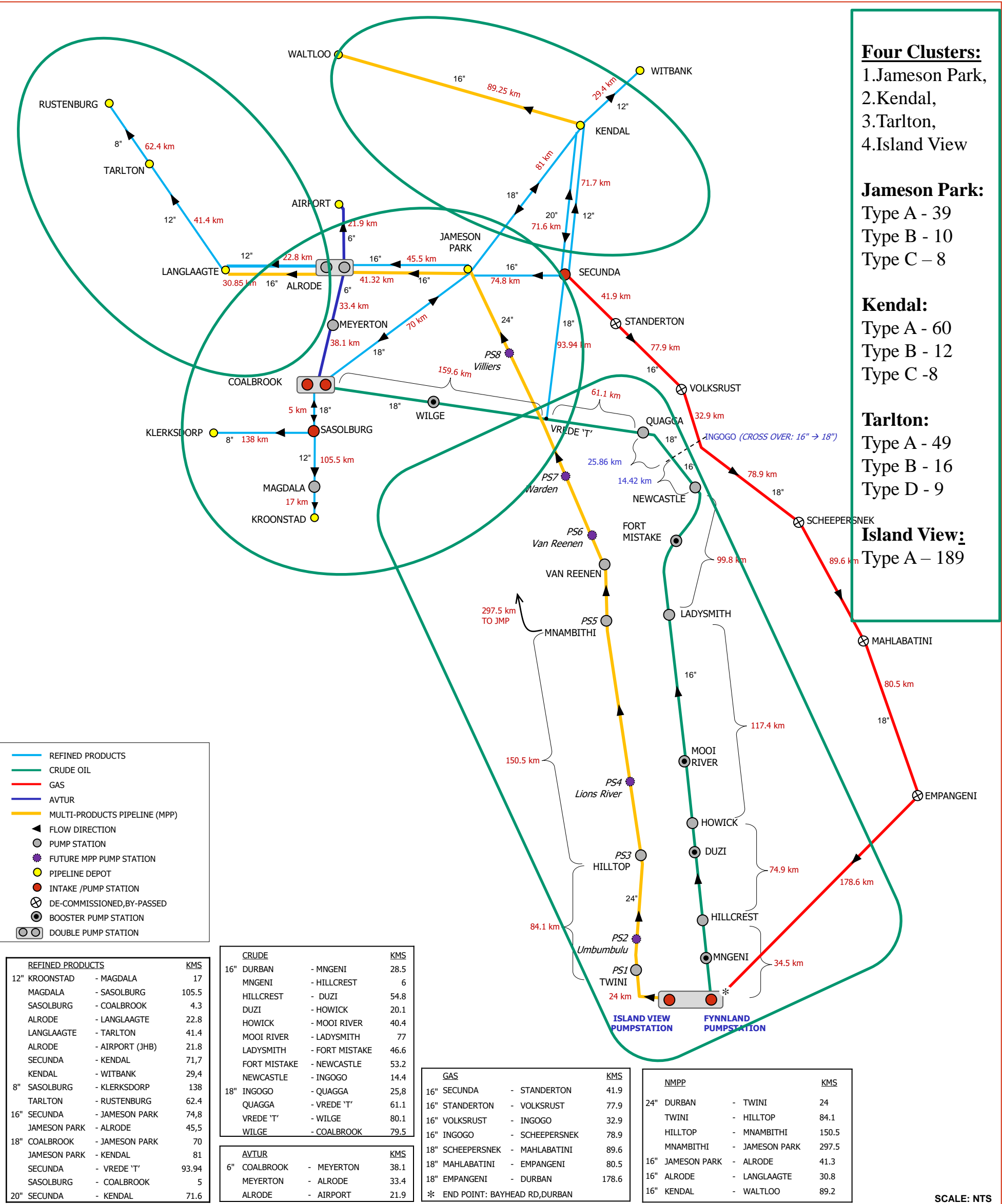


# BLOCK VALVE's LOCATION – ANNEXURE A



TRANSET PIPELINES – PIPELINE NETWORK

BLOCK VALVES AREAS, DISTANCES





## IMAGES OF THE TYPICAL TWO TYPES OF BV'S (ANNEXURE B)

