Transnet SOC Ltd.
Registration
Number
1990/000900/30

13 Girton Road.
Parktown
2193

Private Bag X47
Johannesburg
2000
Tel: 011 584 0509
Fax: 011 774 9978

TRANSNET
freight rail

TPT FUEL FACILITY GAP ANALYSIS

SITES DCT PIER 1 TPT DIESEL DEPOTS

PURPOSE: MAINTENANCE AND HOUSEKEEPING

PURPOSE

1. To provide feedback with the status of the TPT fuel depots with regard to their conditions with regard to maintenance and housekeeping. A request was made by the energy managers at TPT to have the fuel facilities fixed so as to reduce environmental pollution through leaks and worn out equipment

BACKGROUND

2. DCT 1 is a fuel depot, located at the port of Durban. The original installation was by the oil company and managed by them. The requirement and need for the facility was to assist a few diesel run equipment and vehicles so as not to take them off the property for fuel. Due to the lack of maintenance by the oil company Transnet took a business decision to buy back all the facilities and maintain them.

   Transnet Fuel Solutions (TFS) assisted with managing the Fuel Facilities for the group and that included TPT.

DEPOT ASSETS

The site comprises of the following assets

1. 2 x 23 000lt underground diesel tanks
2. 1 x Prowalco single hose pump
3.Concrete slab
4. Operator office with power

DEPOT REPORT

The depot orders consistently approx. 1 x 23 000lt diesel per week. Currently refueling takes place during the day. There are 1 operators that work at the fuel depot. The depot refuels forklifts, generators and mobile bowsers. These mobile bowsers go to the machines and refuel them so as to optimize operations.

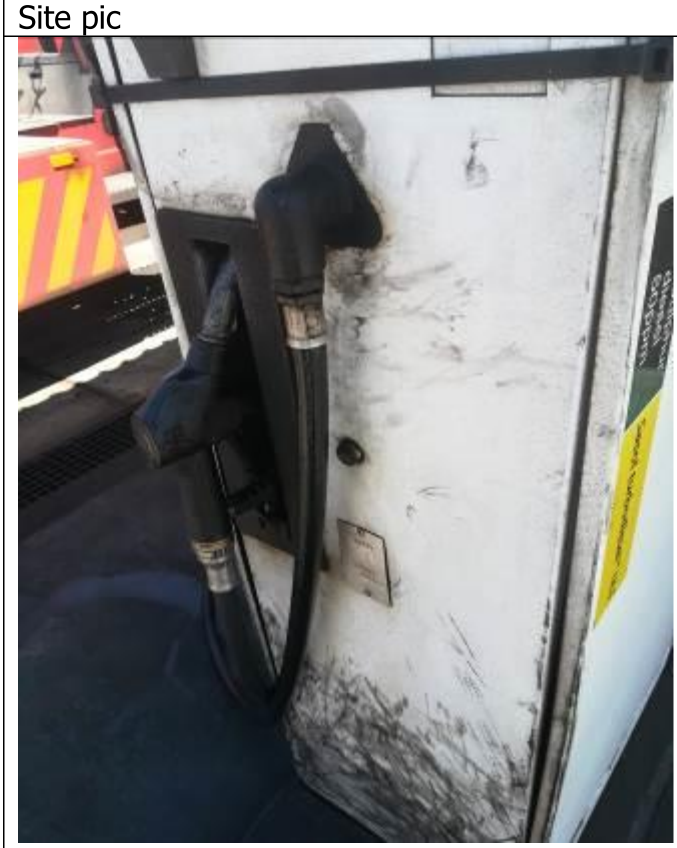
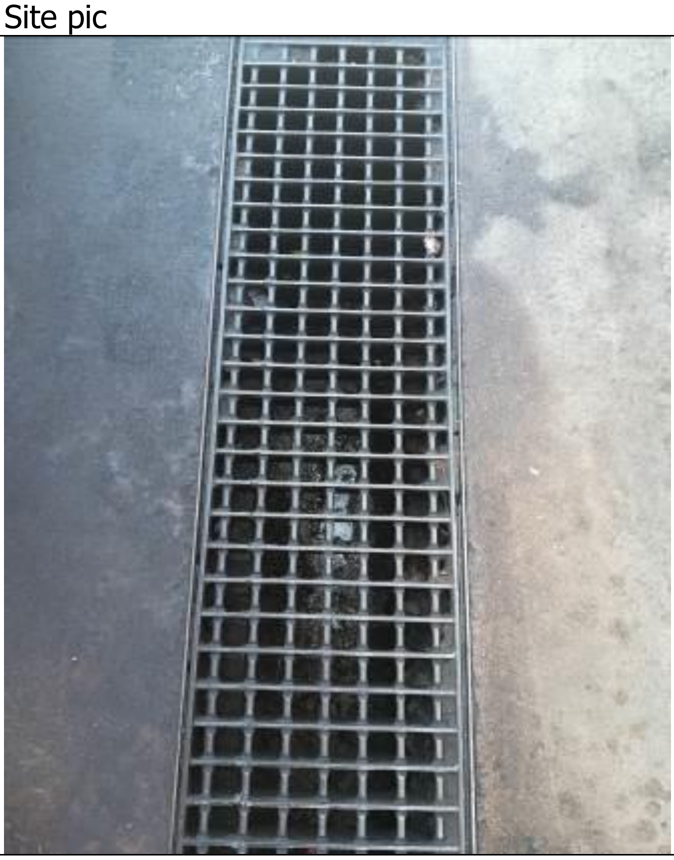
This site is in a very dangerous situation most especially for fuel theft and environmental incidents. The ocean is approx. 10-15mts away. The assumption is that one of the tanks may be leaking. In the event that it is, the diesel can easily make its way to the ocean thereby contaminating the ocean.

Recommendations

A complete redo of the facility. Putting in a 40 000lt self bunded containerised tank. The tank will be fitted with all the requirements of a kerb side pump and a coupling to receive fuel.

For improved management of fuel stock I recommend an improved fuel automation that would connect as follows

1. Record fuel received
2. Record fuel in the tank
3. Identify vehicles with driver and fuel attendant
4. Record KM's and liters received into vehicles
5. Same technology must be fitted onto the mobile bowser
6. This information should be visible by all stakeholders of the depot via a dashboard
7. This information must be captured by SAP

Site pic	Site pic
	
Pump condition	Drainage

Compiled by:

Ebrahim Banoo
Facilitates Manager, TFS SCS
Date: 02 November 2019

Transnet SOC Ltd.
Registration
Number
1990/000900/30

13 Girton Road.
Parktown
2193

Private Bag X47
Johannesburg
2000
Tel: 011 584 0509
Fax: 011 774 9978

TPT FUEL FACILITY GAP ANALYSIS

SITES DCT PIER 2 TPT DIESEL DEPOT

PURPOSE: MAINTENANCE AND HOUSEKEEPING

PURPOSE

1. To provide feedback with the status of the TPT fuel depots with regard to their conditions with regard to maintenance and housekeeping. A request was made by the energy managers at TPT to have the fuel facilities fixed so as to reduce environmental pollution through leaks and worn out equipment

BACKGROUND

2. DCT Pier 2 is a fuel depot, located at the port of Durban. The original installation was by the oil company and managed by them. The requirement and need for the facility was to assist a few diesel run equipment and vehicles so as not to take them off the property for fuel. Due to the lack of maintenance by the oil company Transnet took a business decision to buy back all the facilities and maintain them.

   Transnet Fuel Solutions (TFS) assisted with managing the Fuel Facilities for the group and that included TPT.

DEPOT ASSETS

The site comprises of the following assets

1. 4 x 83 000lt vertical diesel tanks
2. 4 x Prowalco double hose pump on islands
3. Forecourt with forecourt canopy
4. Receiving pump set
5. Decanting pump set
6. Decanting coupling
7. Refueling hose with Wiggins nozzle
8. Bund wall around the tank
9. Operator office with power
10. ATG

DEPOT REPORT

The depot orders approx. 7 x 40 000lt diesel every week. Currently refueling takes place only in the in the day. There is one operator that work at the fuel depot. The depot refuels forklifts, generators and mobile bowsers. These mobile bowsers go to the machines and refuel them so as to optimize operations.

The site has not been upgraded lately. The tanks are in fairly good condition. There are signs of rust forming. It is still early stages if not attended to could cause major damage. The upgrade was only done to the tanks as they were in a very bad condition and was about to rupture. The kerb side pumps need attention. The canopy has a major dent in it and requires repairs. There are rust build up due to neglect. No major maintenance has been done on the site in the last 2 years. Repairs are done if something breaks.

The pumps and flowmeters have not been calibrated in the last year. I found diesel in the receiving hatch for diesel. A pressure test would need to be done to identify a leak. This is a high volume site and a lot more emphasis has to be made on scheduled maintenance and housekeeping.

The pump islands are cracking badly, this could be related to the heavy vehicles fueling. The new islands must be specked to accommodate these bigger heavier vehicles. The tanks over filling is due to faulty ATG probes in the tanks. The current system is very old and outdated it is basically a legacy system that would not be able to service the current demand.

The pump sets need to be serviced as it is visible that they are extremely strained as some have small leaks others have excessive sweat. Due to lack of housekeeping the site looks worse than what it really is. There is a firefighting system installed however nobody on site is trained to use it nor has the system ever been tested since installation.

The oil separator pit needs constant draining and staff need to be trained at monitoring this unit. In the event of overfilling the oil separator the run off can go into the ocean.

Recommendations

The site personnel requires training on the Standard Operating Procedure of working at a fuel facility. The importance of housekeeping must be stressed as this helps with the life span of the equipment. The following maintenance actions need to be implemented

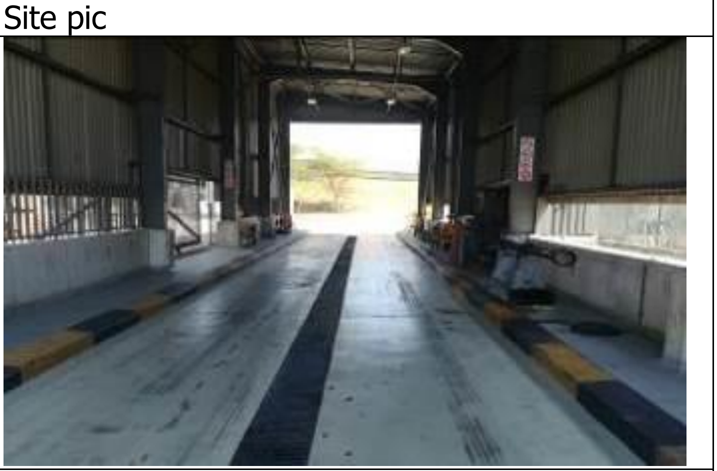
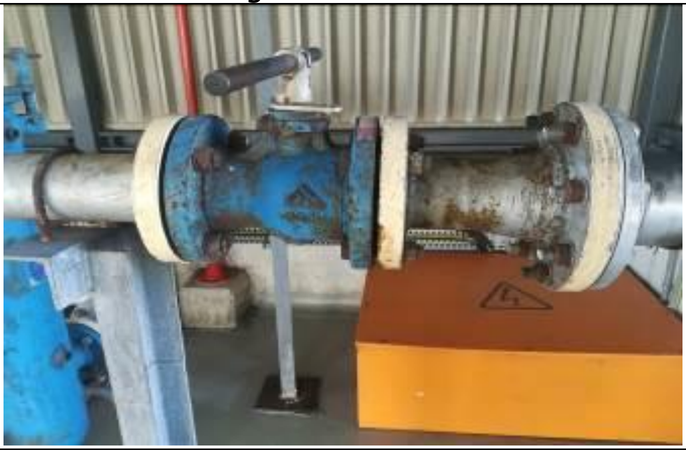
1. Calibration of the pumps and flowmeters
2. Calibration of the pressure gauges
3. New tank strapping done
4. Tank refurbishments. (Good practice at the ports is every 2 years this in return keeps the maintenance cost down on tank maintenance and increases the life of the tanks).
5. The spill drains are blocked these need to be unblocked and kept clean
6. Repair the fuel line where the leaks are taking place.
7. Replace all flange gaskets
8. Pressure test the lines and tanks

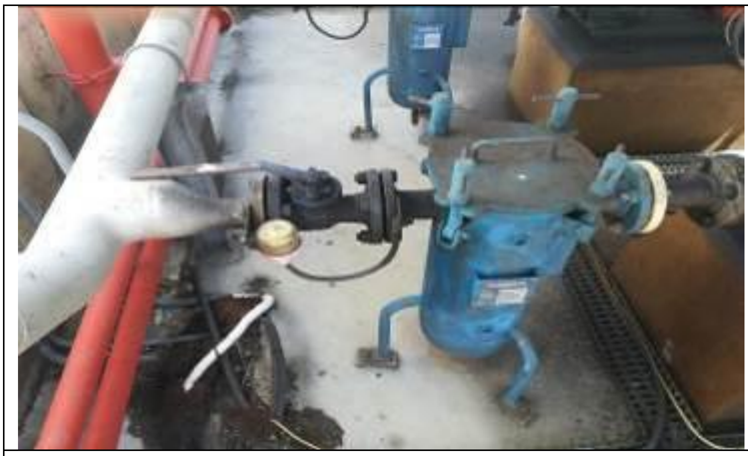
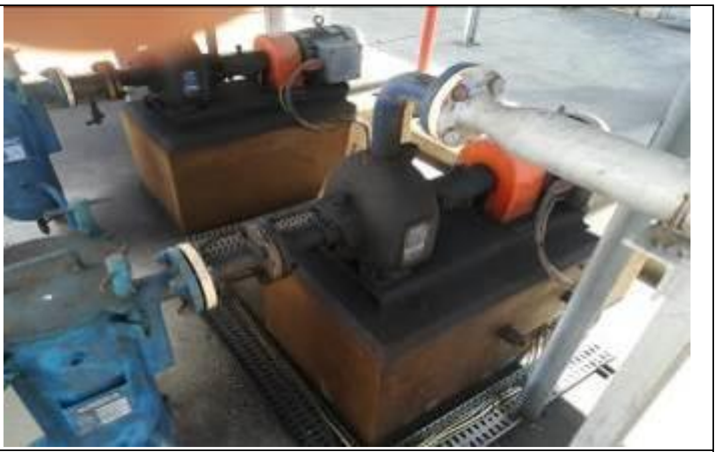
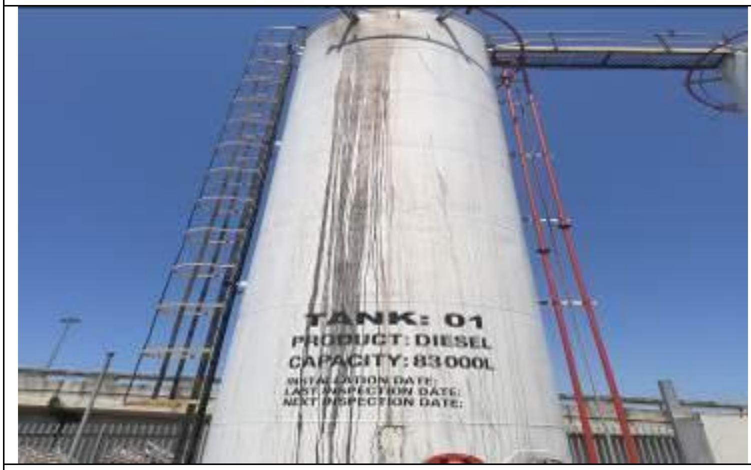
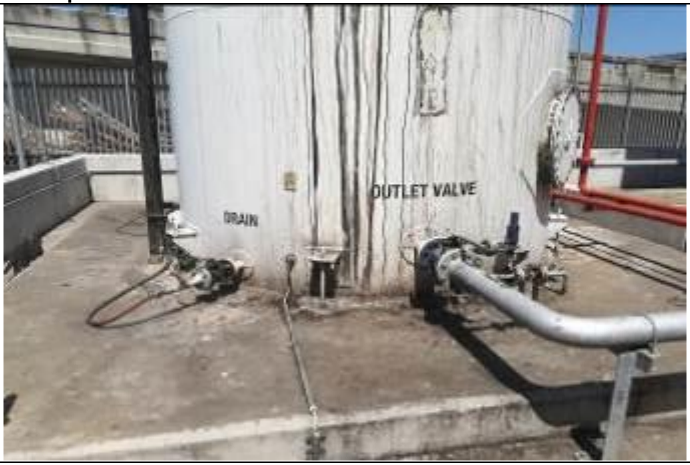
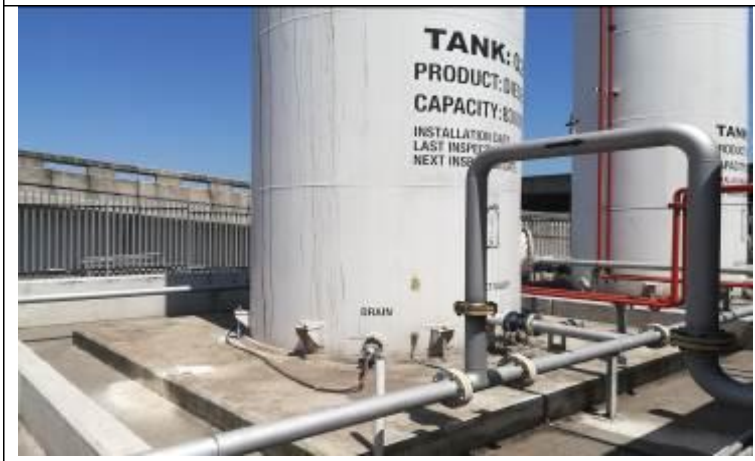
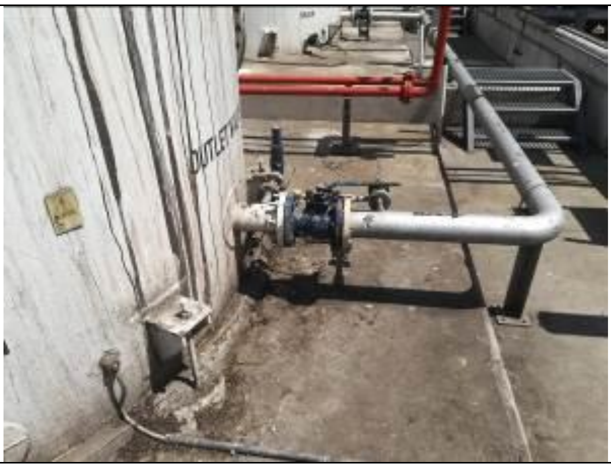
The fire system be handed to the ports local Hazmet to manage and test. The fuel operator should be trained on the basics to start the system in case of fire and to stop the system in case of accidental start.

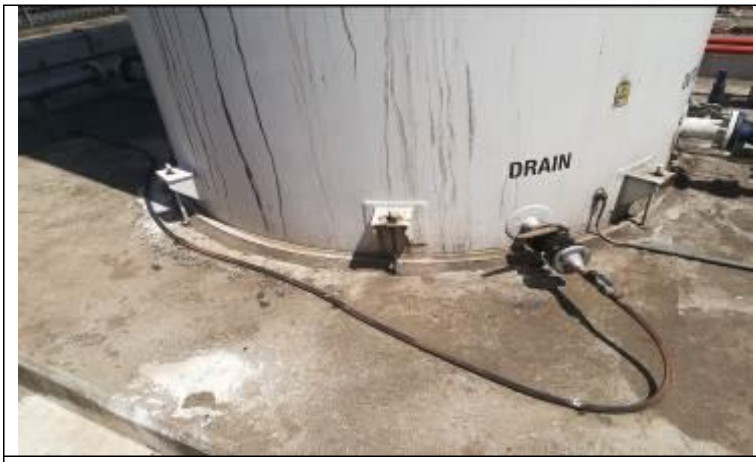
The oil separator needs to be upgraded to a closed system. This system separates the oil and water faster than the current installed system. The water is than clean enough to be sent to storm water. The water may need to be tested before discharging into storm drains.

For improved management of fuel stock I recommend an improved fuel automation that would connect as follows

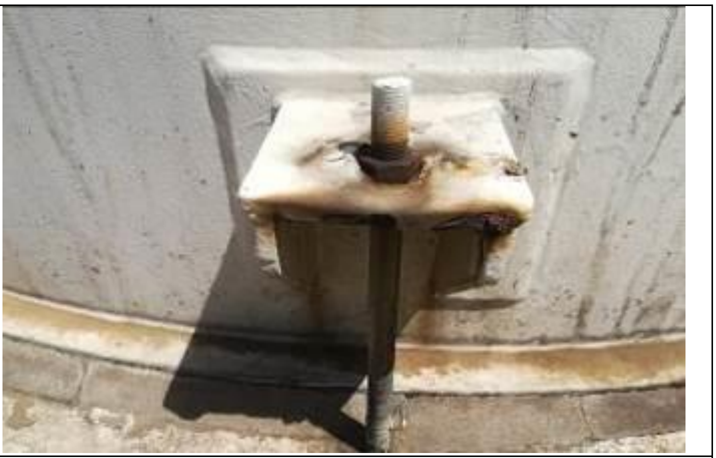
1. Record fuel received
2. Record fuel in the tank
3. Identify vehicles with driver and fuel attendant
4. Record KM’s and liters received into vehicles
5. Same technology must be fitted onto the mobile bowser
6. This information should be visible by all stakeholders of the depot via a dashboard
7. This information must be captured by SAP

Site pic	Site pic
	
Dip point of the tank	Some rust starting to form
	
Refueling and decanting of large vehicles	Valves need attention

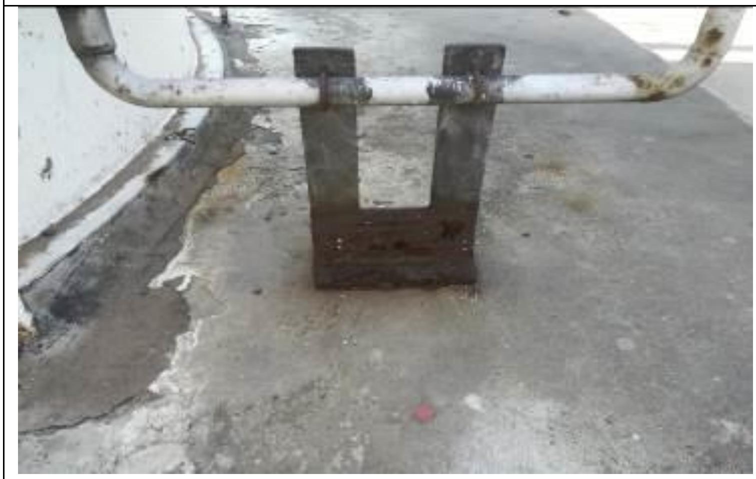
	
Valve and filter	Pump sets need service
 TANK: 01 PRODUCT: DIESEL CAPACITY: 83000L INSTALLATION DATE: LAST INSPECTION DATE: NEXT INSPECTION DATE:	
Tank 1 visible spillage	Tank 1
 TANK: PRODUCT: CAPACITY: INSTALLATION DATE LAST INSPE NEXT INSP DRAIN	
Tank 2 spillage	Condition of valves on the tanks



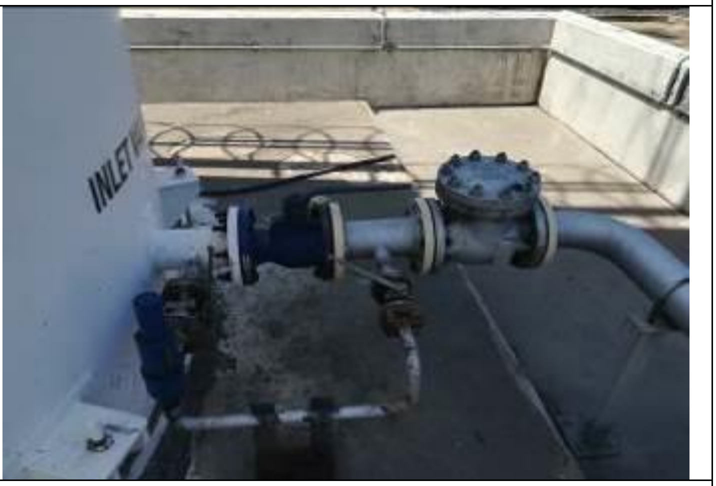
Water bottom valve with hose



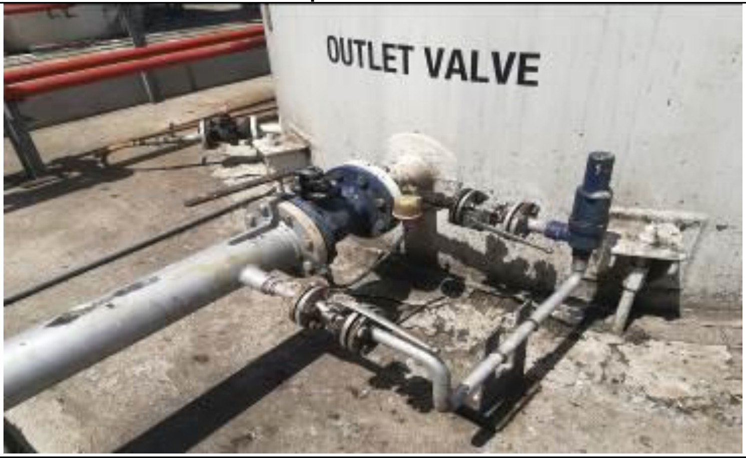
Rusted tank anchor



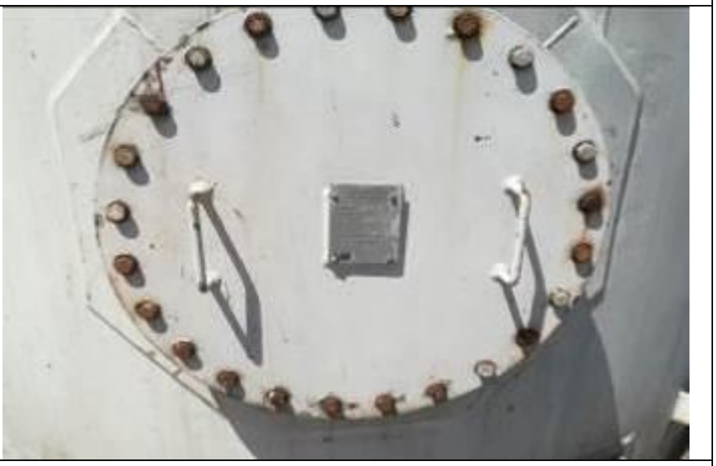
Rusted thermal relief plinth



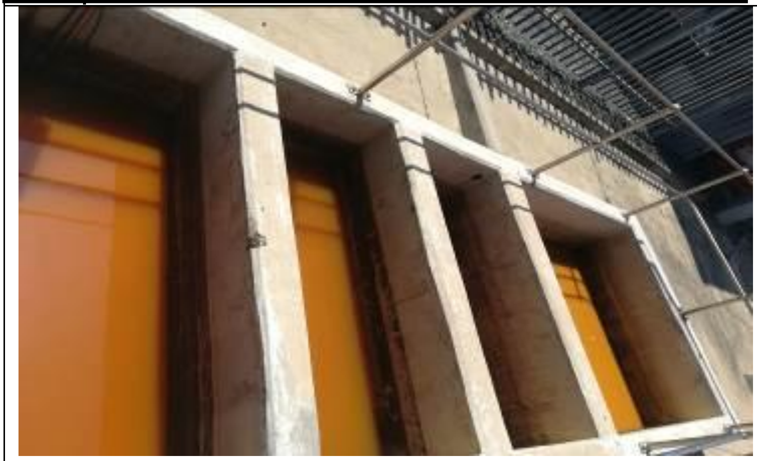
Valves and strainer

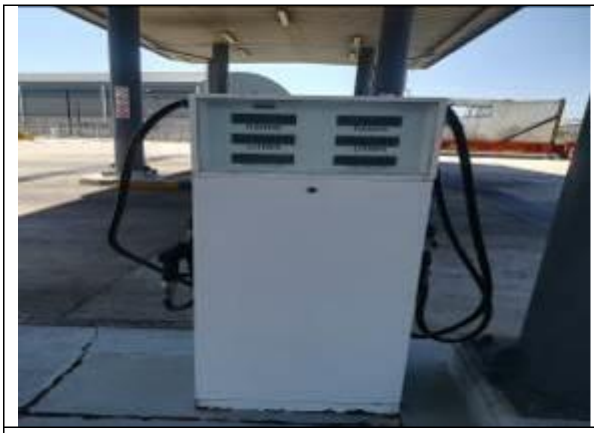
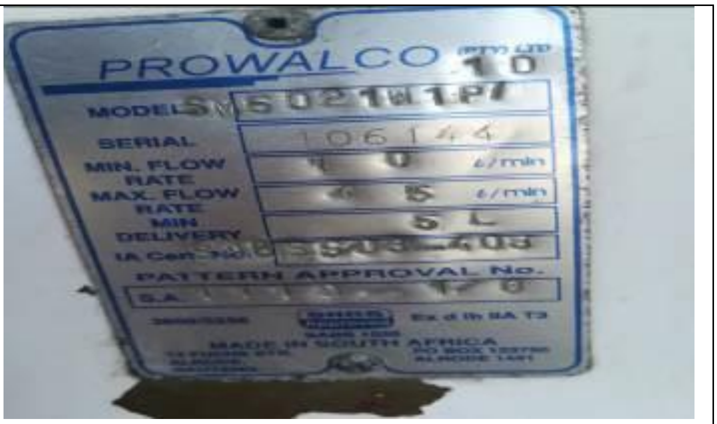
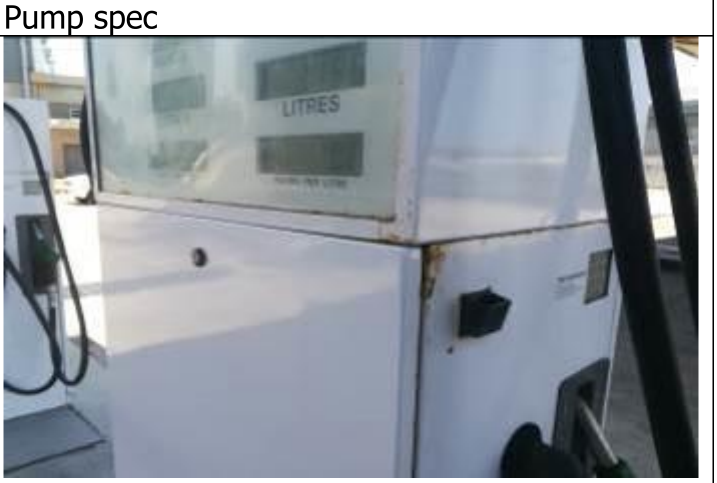
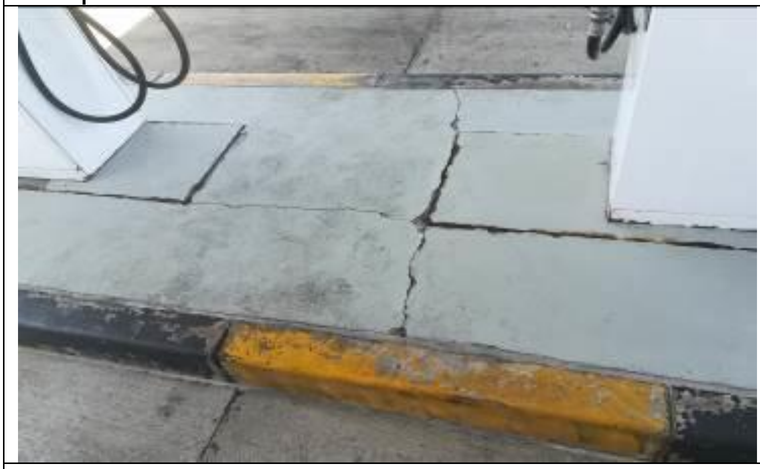


Tank thermal relief



Rusted manhole bolts

[redacted]	[redacted]
	
Oil separator pit needs clean up	Tank farm view
Pumps and filters	Pump station in relation to the tanks

	 PROWALCO (PTY) LTD 10 MODEL SM 5021W1P7 SERIAL 106144 MIN. FLOW RATE 10 ℓ/min MAX. FLOW RATE 45 ℓ/min MIN DELIVERY 5 L IA Cert. No. PATTERN APPROVAL No. S.A. MADE IN SOUTH AFRICA
Prowalco Kerb side pump 2 hose	Pump spec
	
Pump island view	Rust forming on pumps
	
Pump islands badly cracked	Forecourt canopy rusting

ATG printer	Nozzle leaking needs repairs
[redacted]	
[redacted]	Condition of canopy
[redacted]	
[redacted]	Diesel in the receiving line (Leaks)

Compiled by:

____

Ebrahim Banoo
Facilitates Manager, TFS SCS
Date: 02 November 2019

Report Name : Inland Terminal Fuel Facilities - Site Visit Report

Project Number : Z9000113

Document Number :

Prepared by:

Name	Designation	Department	Signature	Date
McDonald Tsubella	Engineering Manager	ECPOT		12/03/2024

Reviewed by:

Name	Designation	Department	Signature	Date
Sphamandla Mathonsi	Senior Project Manager	ECPOT		12/03/2024

Accepted by:

Name	Designation	Department	Signature	Date
Akil Maharaj	Head of Eng, Infrastructure, Energy & Sustainability	ECPOT	A Maharaj	12/03/2024

Table of Contents

Definitions/Abbreviations

NEMA	National Environmental Management Act.
OHS Act	Occupational Health & Safety Act
NFPA	National Fire Protection Association
SANS	South African National Standards
API	American Petroleum Institute.
AIA	Approved Inspection Authority
MHI	Major Hazard Installation
LDV	light duty vehicle
TPT	Transnet Port Terminals

1 Background

TPT Inland Terminals uses diesel to support its operations for export of dry bulk which includes chrome, coal, and manganese. The cargo handling equipment that uses diesel includes pay loaders and light duty vehicles (LDV's).

TPT also noted that the tanks do not have fuel management system in place to account for fuel usage. An audit was conducted across all the terminals from late 2019 to early 2020., of which the audit excluded the inland terminals. The audit focused on capacity adequacy and effectiveness of controls, emergency plans and the current condition of the fuel facilities.

Three inland terminals were visited, and critical issues were identified, and recommendations were provided accordingly.

2 Fuel Facility Assessment

A site visit was conducted across three (3) TPT inland terminals to assess the condition of the fuel facilities. Photographs of noteworthy or pertinent issues were taken, and some of them were used in this report to illustrate the challenges per each site visited. The purpose of the site visit was to establish the condition of the fuel facility and its associated equipment.

The sites visited are shown below in *Table 1 – TPT Inland Terminals*, which also indicates the location and the commodities handled by each terminal.

Table 1 – TPT Inland Terminals

Terminal Name	Location (Province)	Responsible/Managed by	Commodity Handled
Pendoring	North West	Richards Bay Terminal	Chrome
Lohatla	Northern Cape	Port Elizabeth Terminal	Manganese
Kendal	Mpumalanga	Richards Bay Terminal	Coal

2.1 Methodology

The assessment was primarily based on visual inspection of the fuel facilities. Discussions with the operational team onsite were also conducted to understand any existing challenges. Photographs were taken during site visit from each site and used in this report.

3 Findings and Recommendations

3.1 Pendoring Terminal

3.1.1 Findings

The following are findings;

- The terminal does not have a permanent fuel facility.
- The site is using a temporary mobile diesel bowser from external service provider.
- The fuel facility is managed and maintained by an external service provider.
- There is a soil contamination adjacent to the bowser caused by diesel spillage.
- No fire extinguisher on the diesel bowser or nearby vicinity.
- An elevated diesel steel tank shown below (Figure *1: Pendoring Terminal – Temporary External Service Provider Fuel Facility*) is not in use. The tank belongs to an external service provider that previously managed the facility, the tank to be taken off site.

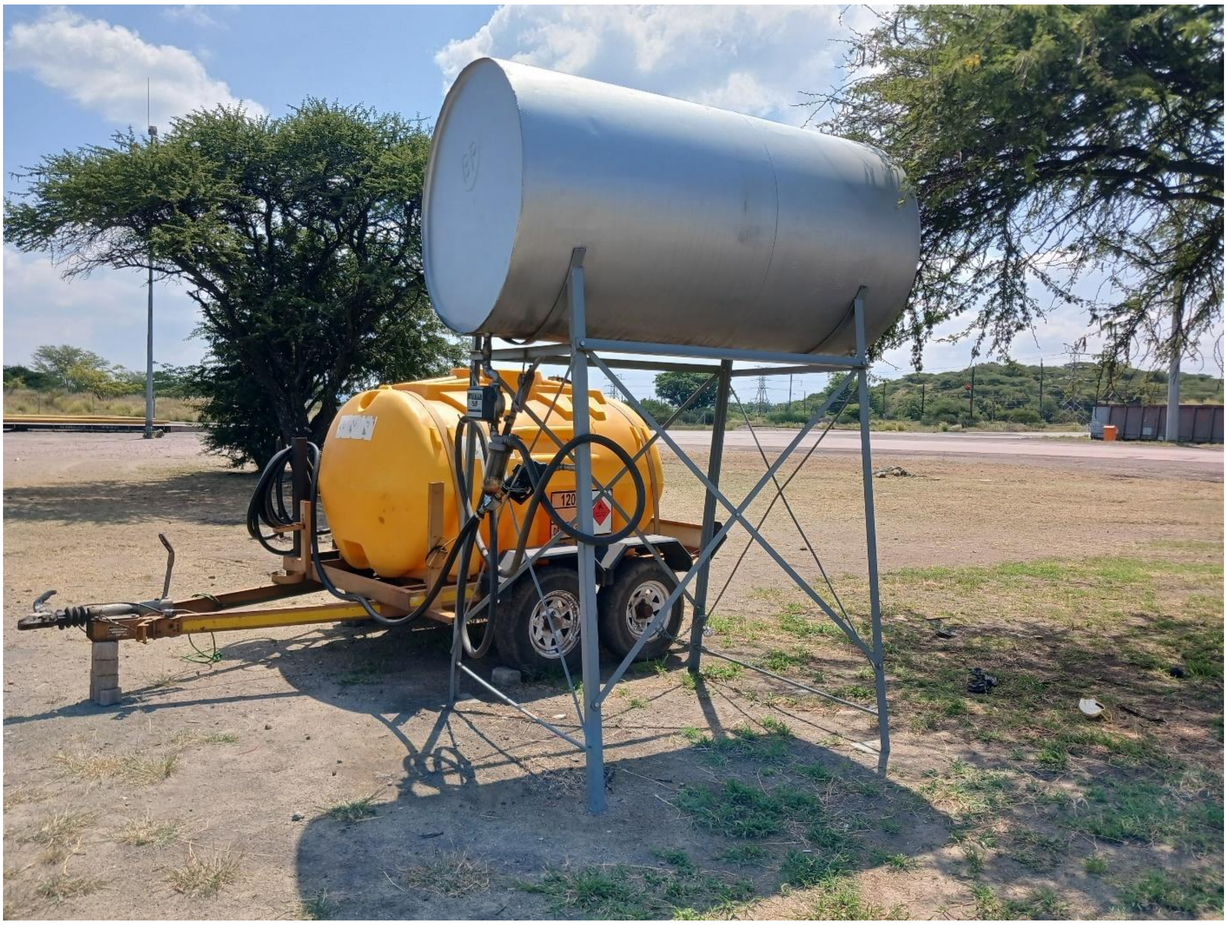


Figure 1: Pendoring Terminal – Temporary External Service Provider Fuel Facility.

3.1.2 Recommendations

The following are recommendations;

- Conduct environmental assessment to ensure compliance
- Conduct risk assessment
- A permanent fuel facility that can be easily decommissioned (i.e., self-bunded tank with a concrete slab).

3.2 Lohatla Terminal

3.2.1 Findings

The following are the findings;

- There are two fuel facilities onsite with two diesel tanks.
- The containerised self-bund tank belongs to TPT and the skid-mounted tank belongs to an external service provider that previously managed the facility (*see below Figure 2 : Lohatla Fuel Facility*).
- The TPT containerised self-bund tank diesel pump is not working.
- Currently the operations are using external service provider fuel facility.
- There is no oil separator or drainage system at the facility to handle spillages.

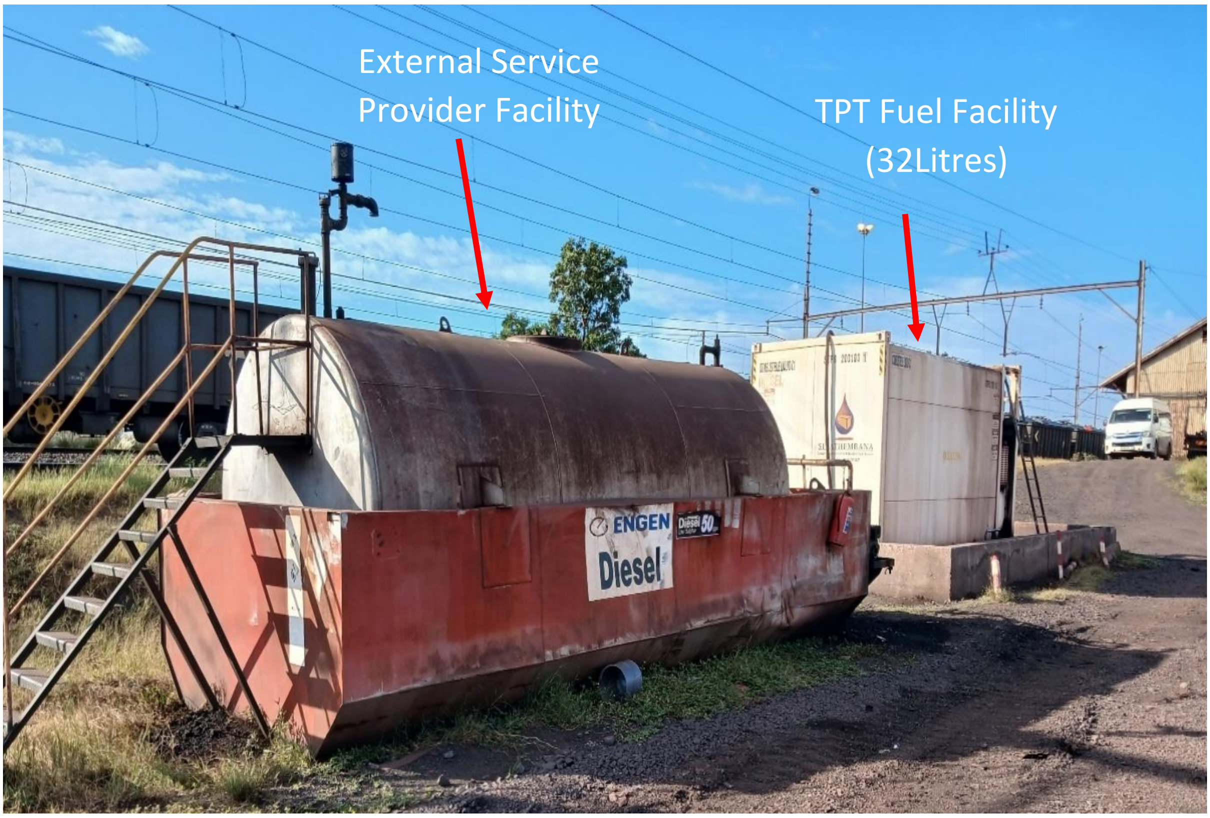
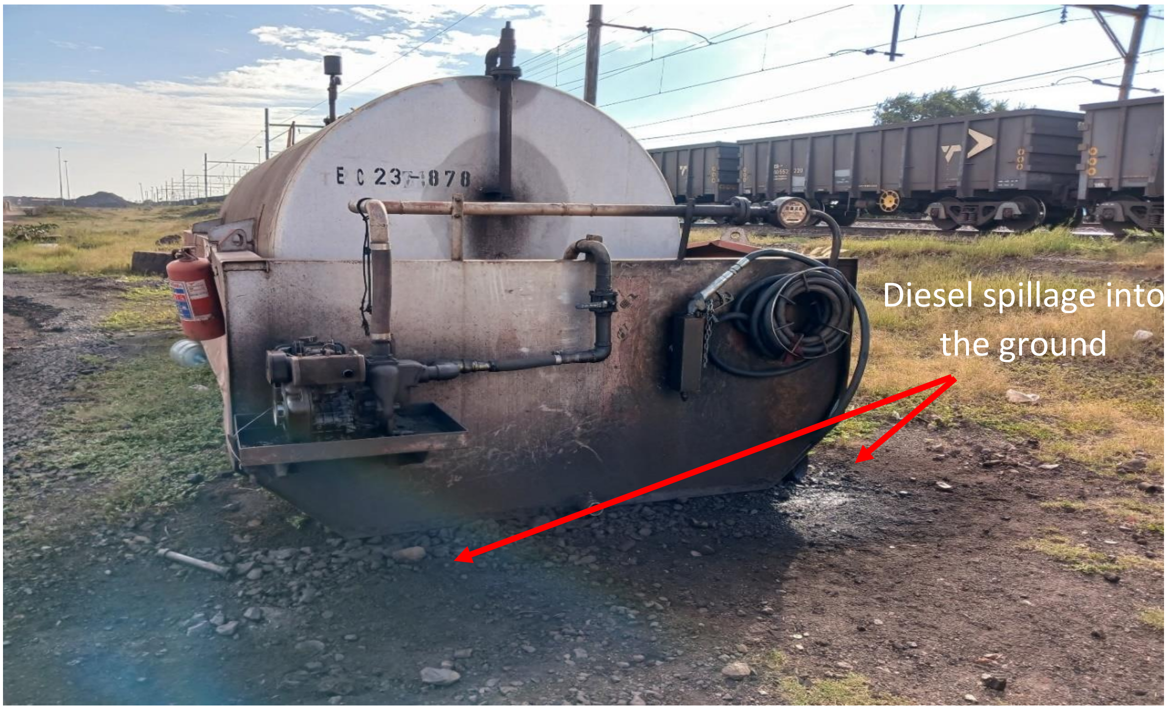
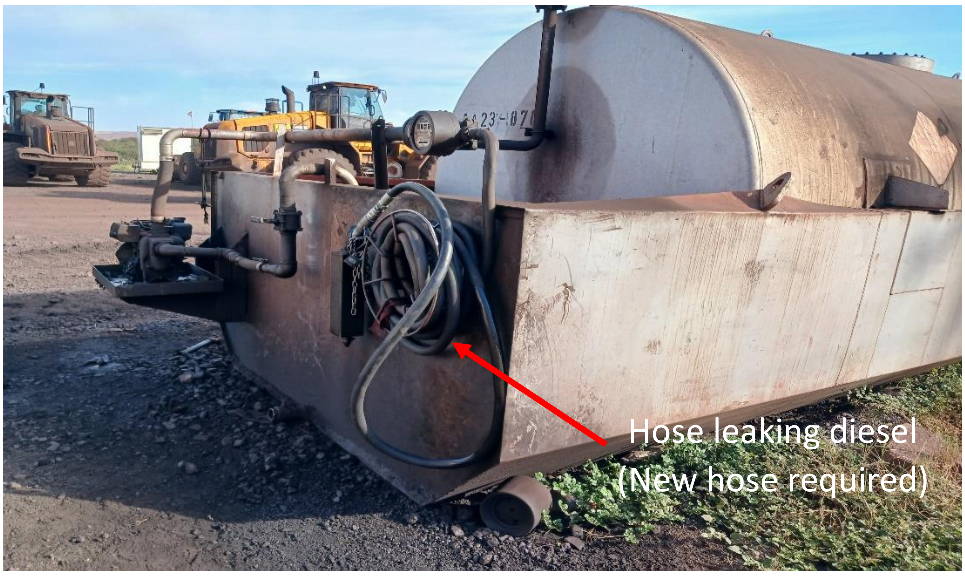
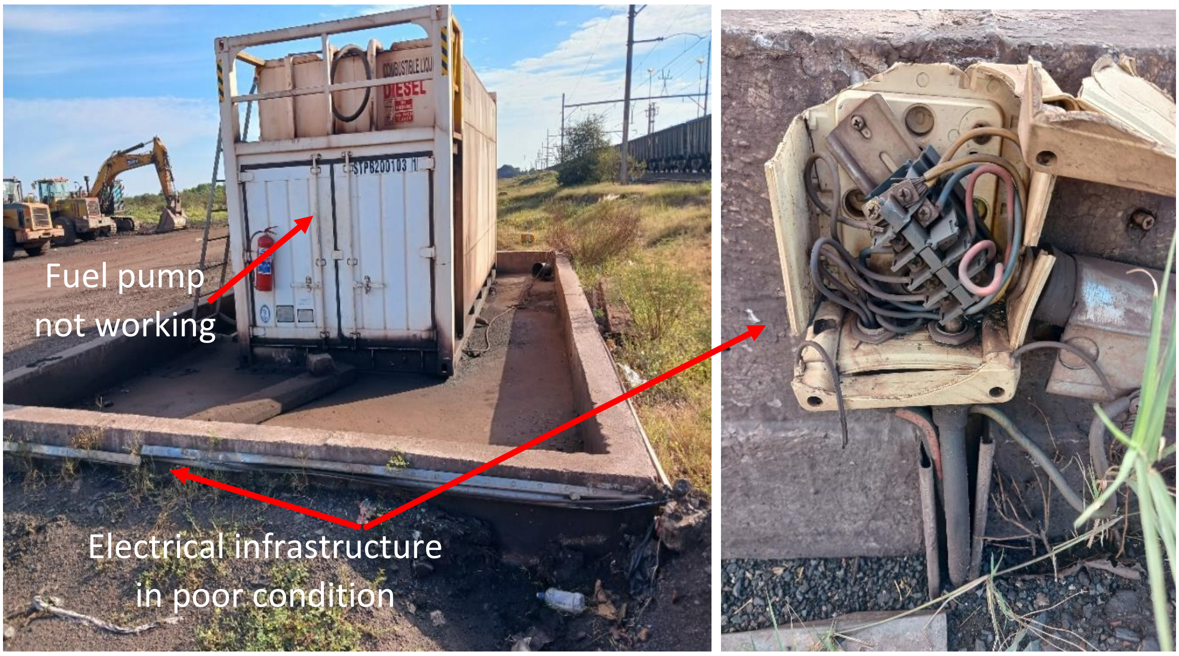

External Service Provider Facility
TPT Fuel Facility (32Litres)
ENGEN
Diesel

Figure 2: Lohatla Fuel Facility

Summary of condition of the fuel facility during the site inspection on 29 February 2024, as illustrated by the following sample photographs below;

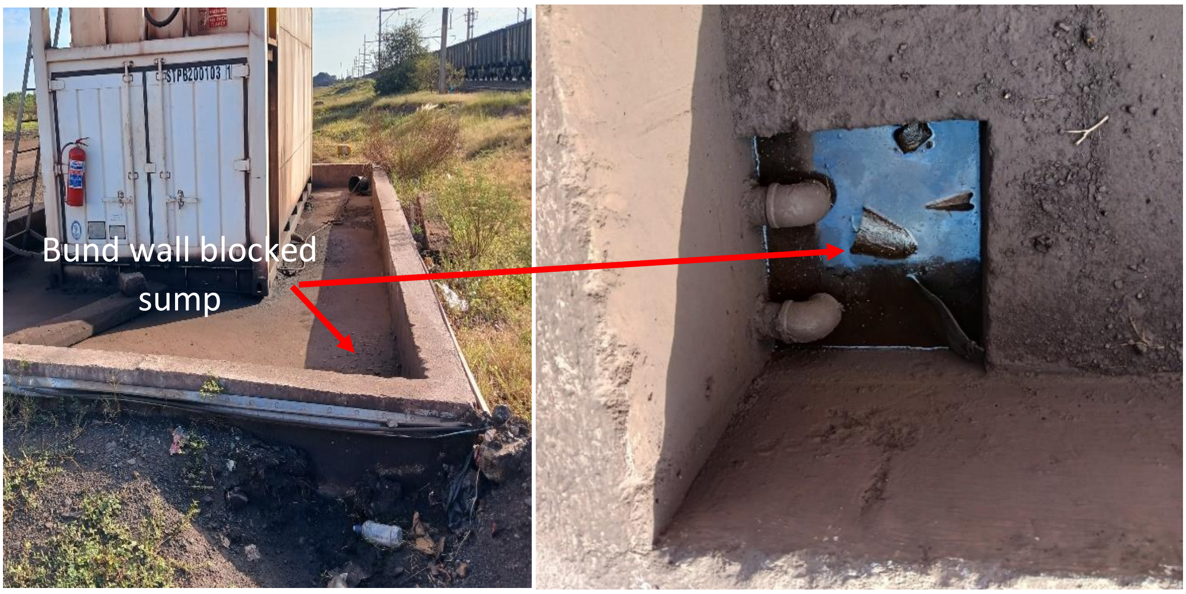

Diesel spillage into the ground

1	**Focus Area**	Fuel Facility – External Service Provider

<table>
<tr><td colspan="3"> </td></tr>
<tr><td><b>2</b></td><td><b>Focus Area</b></td><td>Fuel Facility – External Service Provider</td></tr>
<tr><td colspan="3">

Fuel pump
not working
Electrical infrastructure
in poor condition

</td></tr>
<tr><td><b>3</b></td><td><b>Focus Area</b></td><td>TPT Containerised Self-Bund Tank Fuel Facility</td></tr>
</table>

		
4	**Focus Area**	TPT Containerised Self-Bund Tank Fuel Facility

3.2.2 Recommendations

- The containerised self-bund fuel storage tank and fuel pump requires urgent maintenance and repairs to bring it up to standard.
- Improve general housekeeping to minimise diesel spillages around and within the facility.
- It is recommended that new drainage infrastructure be installed to ensure environmental compliance.

3.3 Kendal Terminal

3.3.1 Kendal Findings

The following are findings;

- The terminal does not have a permanent fuel facility.
- The site is using a rental mobile diesel bowser (2000 litre capacity).
- The terminal has a high diesel run out risk exposure that is caused by limited tank capacity of 2000 litres that require regular diesel top-ups.
- The terminal is experiencing high fuel delivery frequency throughout the month, which is affecting the operations negatively because at times the supplier can’t keep up with small volume deliveries.

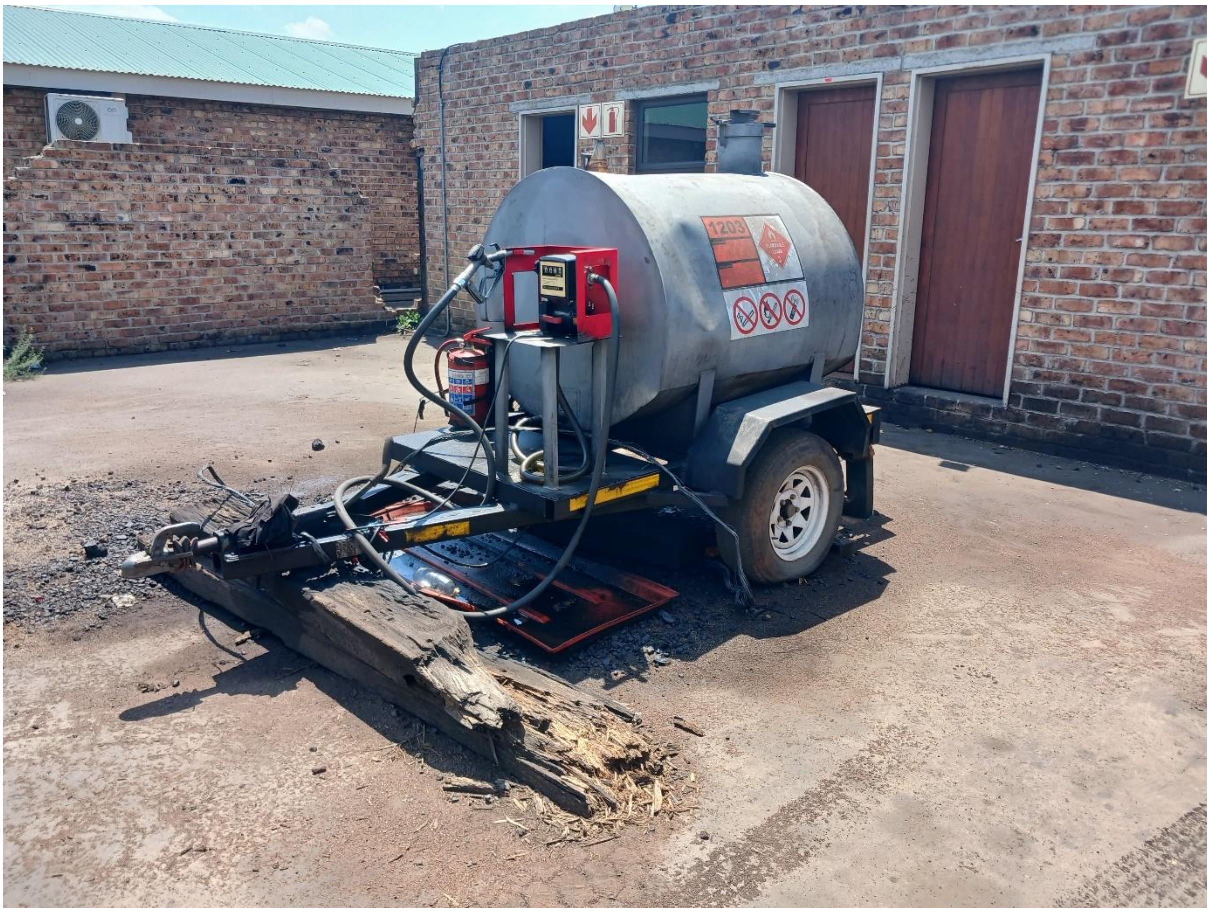
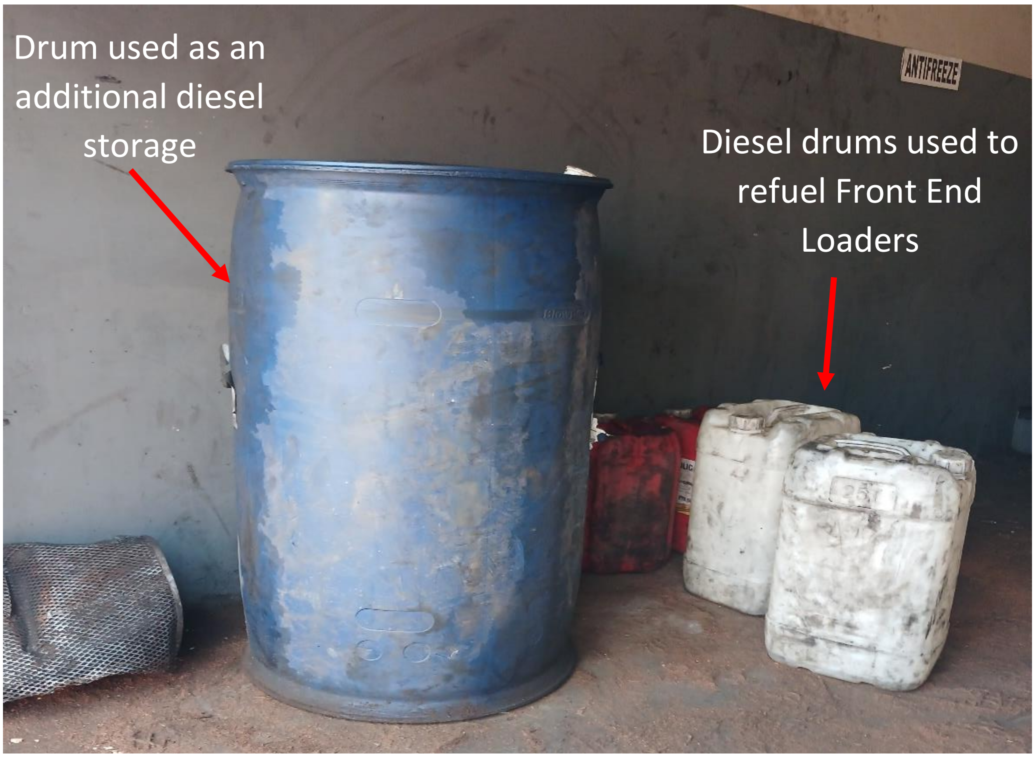
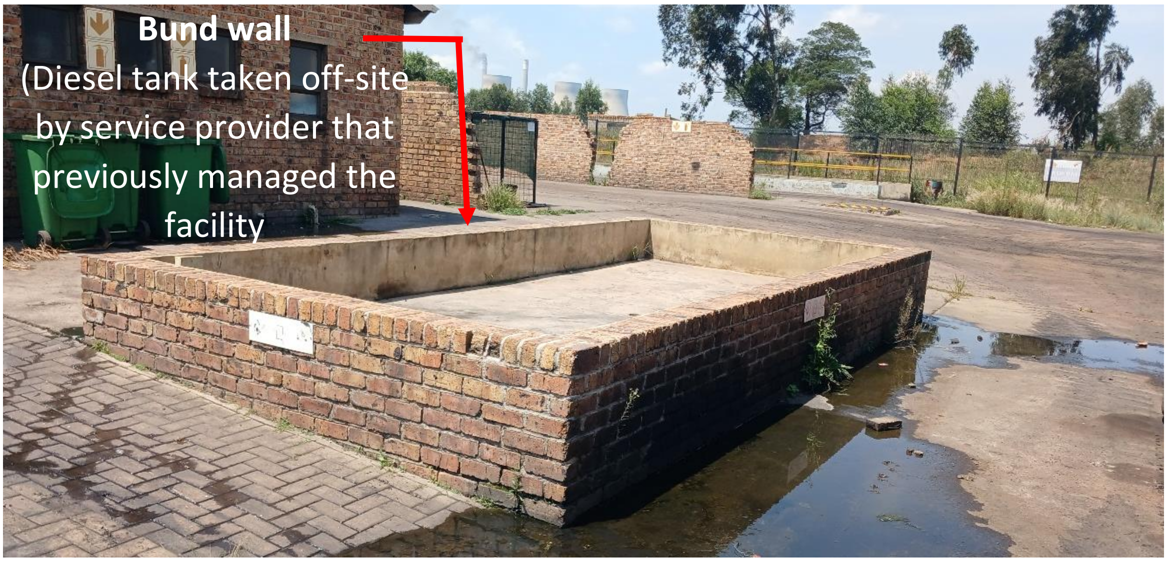


Figure 3: Kendal Terminal – Rented mobile diesel bowser.

Summary of condition of the fuel facility during the site inspection on 01 March 2024, as illustrated by the following sample photographs below;


Drum used as an additional diesel storage
ANTIFREEZE
Diesel drums used to refuel Front End Loaders

5	**Focus Area**	Kendel Fuel Facility – Drums used for refuelling Front End Loaders


Bund wall
(Diesel tank taken off-site by service provider that previously managed the facility

6	**Focus Area**	Kendel Fuel Facility – Bund wall (Used by previous service provider)

3.3.2 Recommendation

- Install a permanent fuel facility (i.e., containerised self-bunded tank).

- For the interim solution, increase the size of the rented mobile bowser to at least 5000 litre capacity.
- Consider reusing the existing bund wall to place a suitable sized containerised self-bund tank.

4 Conclusion

From the site visits conducted across all the three (3) Inland Terminals fuel facilities, it is concluded that all the fuel facilities do not comply in various aspects in accordance with Occupational Health & Safety Act, SANS and NEMA.

The current condition of the inland terminal fuel facilities are in poor condition and pose a potential risk to the operations, as well as the health and safety of personnel. Therefore, it is recommended that the following should be carried out at each of the three inland terminal fuel facilities;

- Install permanent fuel facilities in terminals where they are using temporary rented mobile diesel bowsers.
- Mechanically perform condition assessment according to South African National Standards (SANS) and Approved Inspection Authority (AIA).
- Perform maintenance and critical repairs, obtain compliance certificates, and get the tank registered with the council and energy department.
- Ensure compliance to Occupational Health & Safety Act, SANS and NEMA across all the inland terminals.

PRELIMINARY CONDITION ASSESSMENT

FOR FUEL STORAGE TANKS – PHASE 1

TPT SITE VISIT REPORT COMPLETED IN AUGUST 2022

DOCUMENT REVIEW & ACCEPTANCE

Compiled by:

____

Amit More
Tank & Petrochemical Specialist
Date:

Reviewed by:

____

Yanga Ralarala
Project Manager
Date:

Reviewed by:

____

McDonald Tsubella
Engineering Manager
Date:

Accepted by:

____

Sphamandla Mathonsi
Project Execution Lead
Date: 28/09/2022

1. CONTENTS

2. DEFINITIONS & ABBREVIATIONS

a) NEMA – National Environmental Management Act.

b) OHS Act – Occupational Health & Safety Act.

c) NFPA – Standard on Fire Department Occupational Safety, Health and Wellness Program.

d) SANS – South African National Standards.

e) API – American Petroleum Institute.

f) Approved Inspection Authority (AIA).

g) MHI – Major Hazard Installation.

3. BACKGROUND

TPT has fuel tank facilities across all the terminals to service the equipment and 90% of the facilities were inherited from Transnet Fuel Solutions in 2014. The only facilities that TPT has own from inception is in Nqura Container Terminal and DCT Pier 2. When TPT took over the tanks there was no maintenance plans that were put in place and followed accordingly. Some terminals have been doing minimal maintenance requirements i.e., performing pressure testing; however, this is not enough to ensure that the tanks are fully compliant. Generally, the tanks are now smaller compared to fleet size and increase diesel demand, the tanks are old and non-compliant to Occupational Health & Safety Act, South African National Standards (SANS) and National Environment Management Act National Environment Management Act NEMA.

4. PRELIMINARY CONDITION ASSESSMENT

A preliminary condition assessment that focused on engineering requirements was conducted across all the terminals. The purpose of the assessment was to establish the condition of the tanks, compile scope of work that will be used to appoint the AIA.

Approved Inspection Authority will:

- Mechanically perform condition assessment according to South African National Standards (SANS) and Approved Inspection Authority (AIA).
- Perform critical repairs, obtain compliance certificates, and get the tank registered with the council and energy department.

- Ensure compliance to Occupational Health & Safety Act, SANS and NEMA.

This preliminary condition assessment can be read in conjunction with audits that were conducted by environmental department, energy department and Transnet Fuel Solutions.

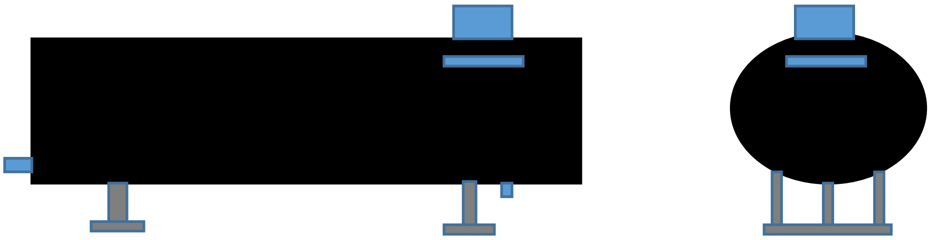
5. TERMINALS

Physical inspections were performed in all Port Terminals. The Current capacity and installation type for each terminal is depicted in the table below:

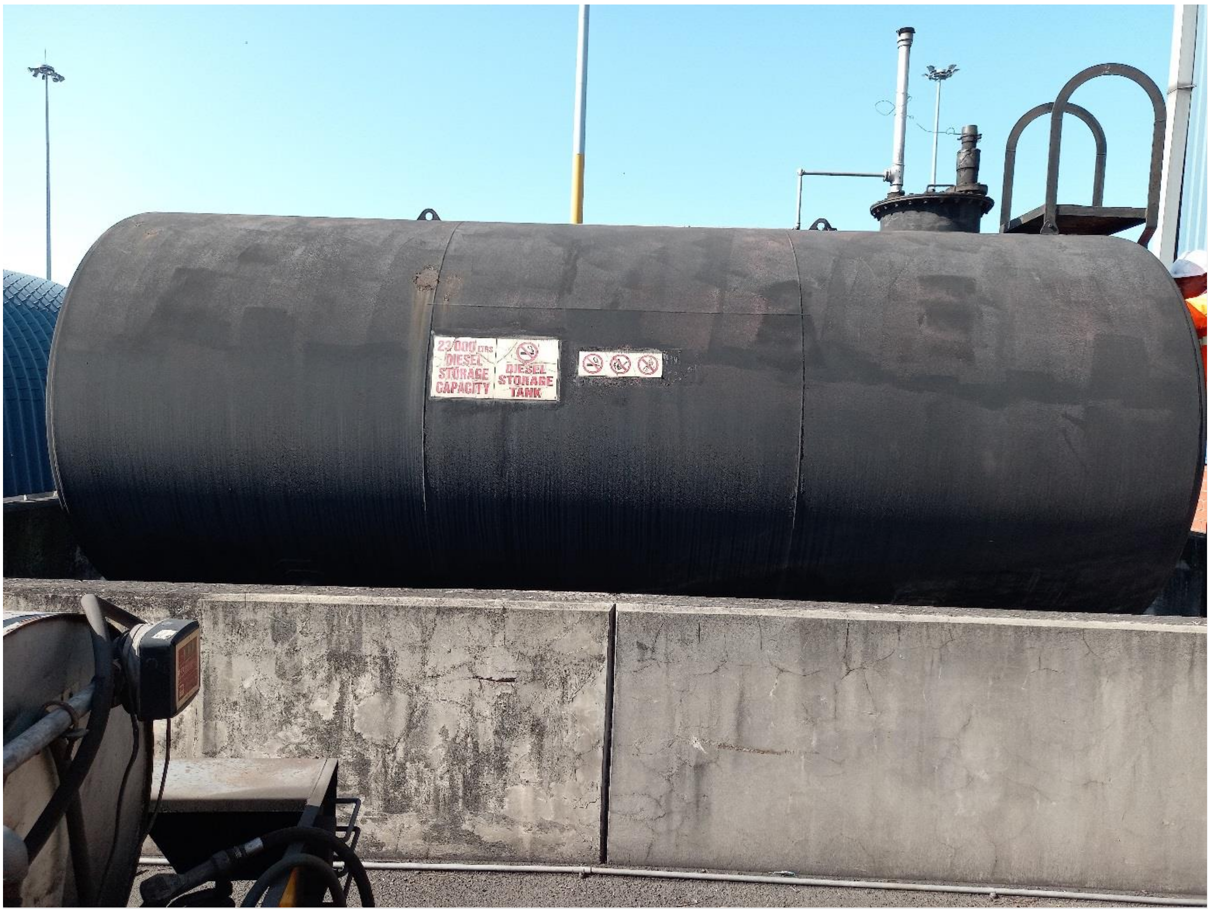
#	Terminal	Capacity & Fuel Type	Installation Type	Tank Hire
1.	Cape Town	2 x 39 000 = 78 000L	Above ground	No – Multiple tanks available
2.	Saldanha	1 x 23 000 = 23 000L	Above ground	Yes – 23 000L
3.	Ngqura Container Terminal (NCT)	4 x 83 000 = 332 000L	Above ground	No – Multiple tanks available
4.	Port Elizabeth	2 x 23 000 = 66 000L	Above ground	No – Multiple tanks available
5.	East London	2 x 23 000 = 66 000L 1 x 14 000 = 14 000L (Discontinued)	***Underground***	No - Existing tanks to be decommissioned once the new installation is completed
6.	DCT, Pier 2	3 x 83 000 = 249 000L	Above ground	No – Multiple tanks available
7.	DCT, Pier 1	2 x 23 000 = 46 000L	***Underground***	No – Existing tanks to be decommissioned once the new installation is completed
8.	Maydon Wharf/ Agri-port	1 x 23 000 = 23 000L	Above ground	Yes – 23 000L
9.	Durban Point	1 x 23 000 = 23 000L	Above ground	Yes – 23 000L
10.	Richards Bay	1 x 63 000 = 63 000L	Above ground	Yes – 65 000L

6. FINDINGS

6.0 DURBAN, MAYDON WHARF



Dimensions of the Tank (2.2 m Diameter X 5.5 m Long)

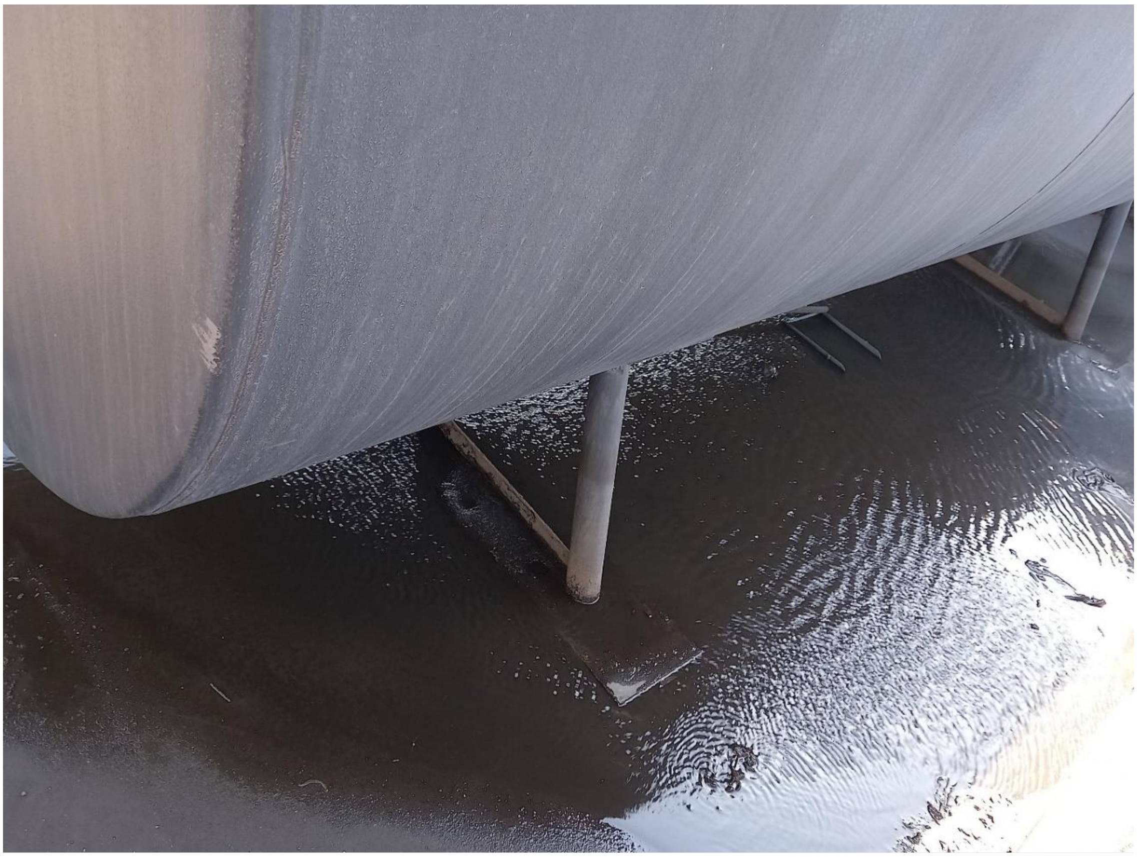


Photograph of the Tank inside the Bund on site

TANK

- One horizontal tank with 23 000 L capacity.
- Tanks has flat ends.
- Corrosion is severe on the Tank at various places.
- Coating / Painting is in a poor condition.

- Base Plate of the support is in the oily storm water and is rusting heavily.
- Tank manufactured by Forgeweld Engineering (PTY) LTD.
- Gaskets needs to be replaced.
- Level Gauge needs to be installed, as currently level is checked by dip stick.



Base plate and supports are getting corroded in the storm water

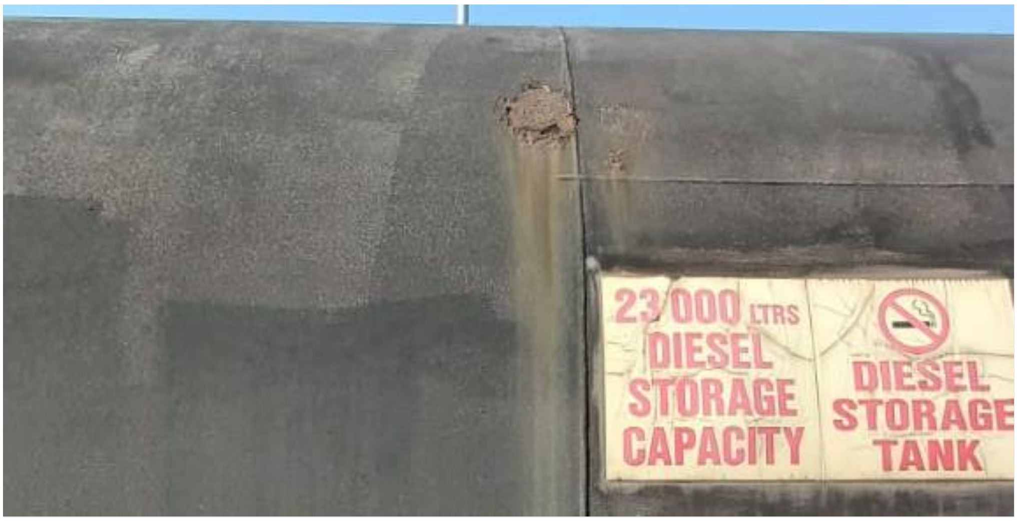


Photo of a corrosion on the Tank

PIPING

- Piping was in an average condition and requires to be painted.
- Handles for the valves were corroded.

ELECTRICAL

- Distribution Board / Electrical connections need to be improved and reinstalled.

INSTRUMENTATION

- All instruments need to be tested.
- Dip Stick to be replaced with level gauge.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder and top landing platform need coating at several areas.
- No stairs and railing to enter the bund area.

CIVIL WORKS

- Bund walls are cracked.
- Distance from Bund wall to Tank does not comply.
- No arrangements are made for diesel Spillage.
- No arrangements are made for storm water drain.
- Bund area was not clean.
- Vegetation was found around the bunded area.

FIRE FIGHTING SYSTEM

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

PUMP

- No maintenance reports or records was found on pumps.

RISK ASSESSMENT

- Risk assessment to be conducted for the entire Tank and the premises.

OIL SKIMMER

- Oil Skimmer and underground Oil spillage drain was not in a working condition.

- Cover was rusted severely at some locations.

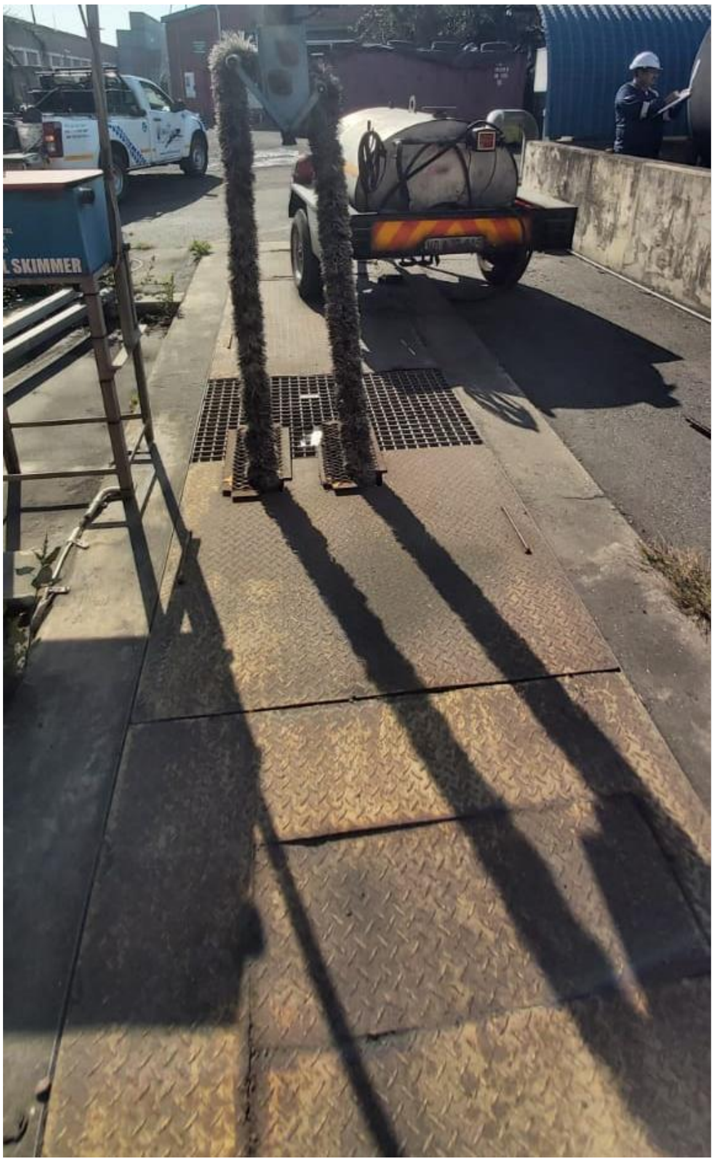
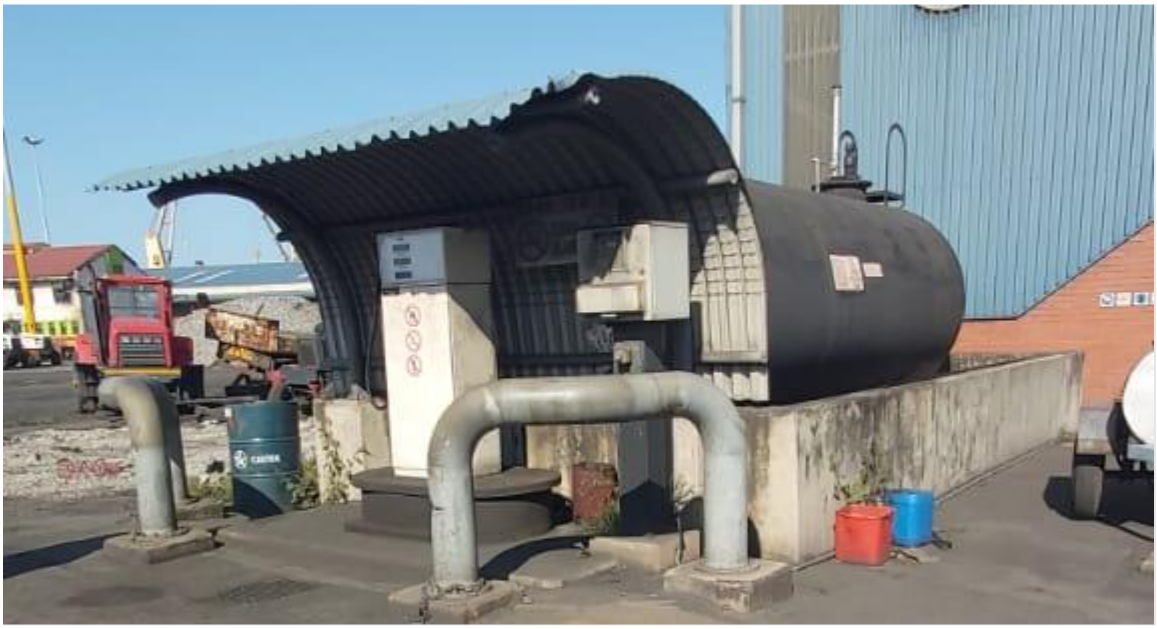


Photo of Rusted Oil Drain Cover

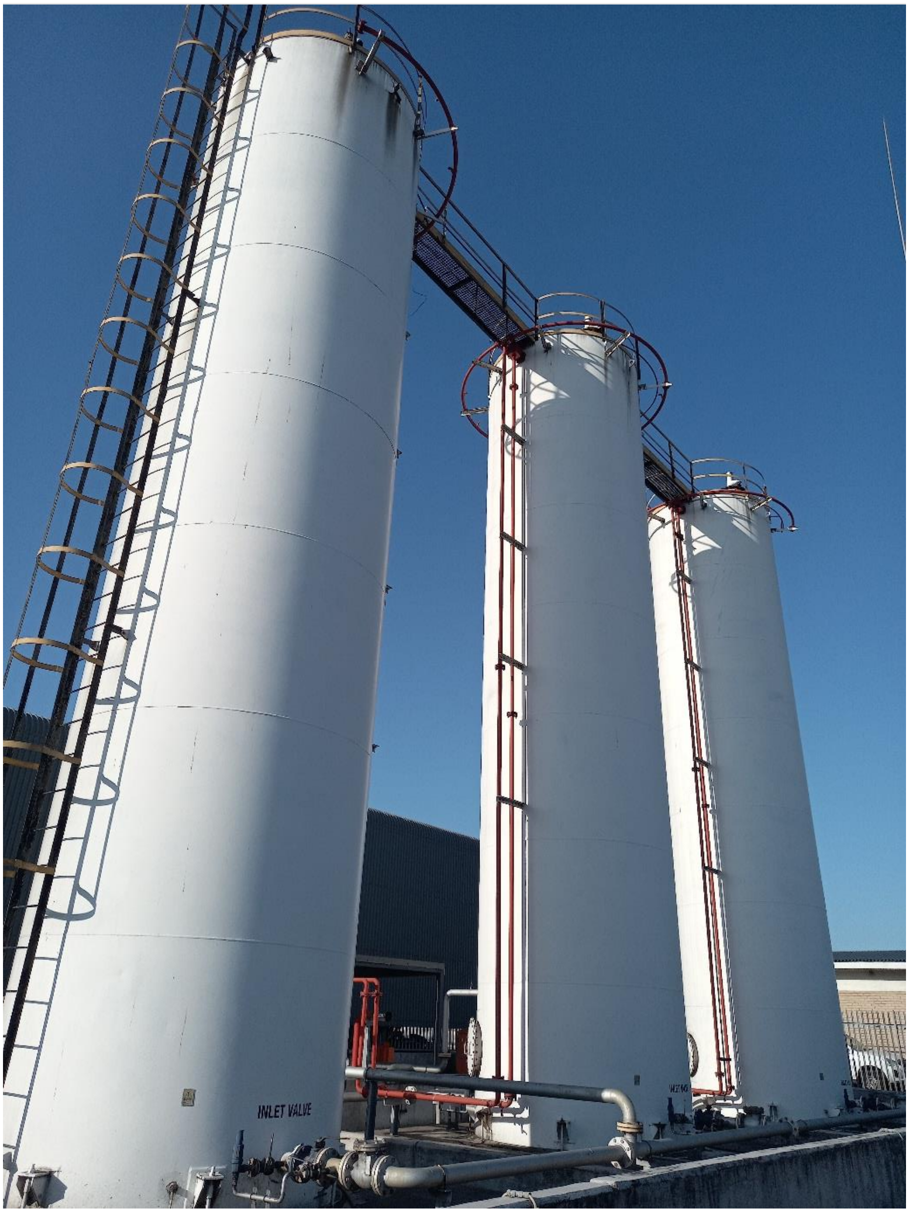
GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required in the area.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.

- No record for calibration of instruments was found.
- No record of operation or maintenance for the facility was found.
- No Drawings, Data books or certificates found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Bund walls are damaged.
- Isolation valves don’t have service history.
- Missing earth wires.
- No electrical compliance certificates.
- Tanks are currently not constructed in accordance with SANS specification for petroleum storage.



6.1 DURBAN, PIER 2

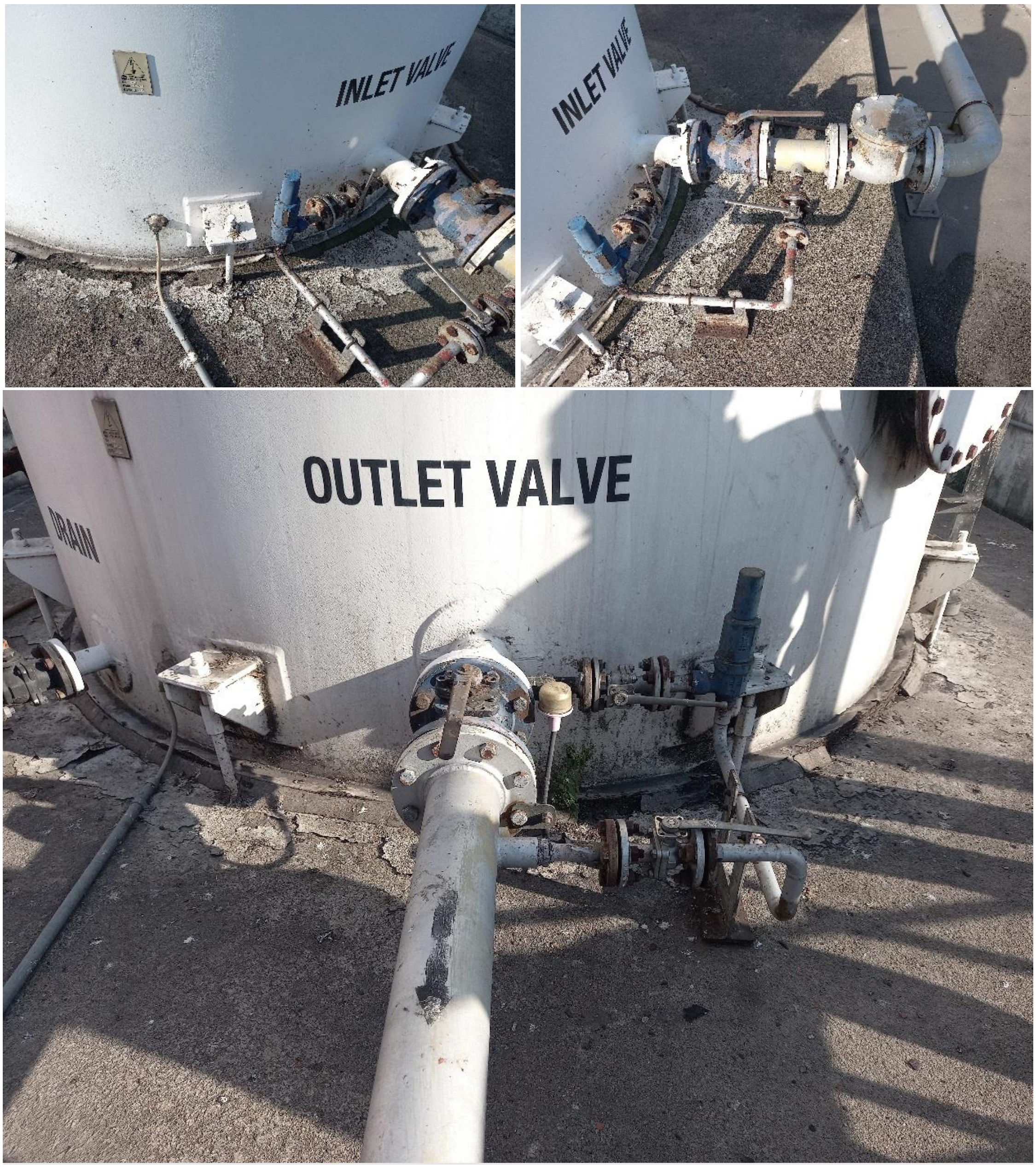


Tank Size: 915 mm diameter x 12.6 meter high: (3 Tanks)

TANKS

- Three 83 000 L Vertical aboveground Tanks were found on site including piping and other accessories.
- Manufactured by Springbok Tank Manufacturing.

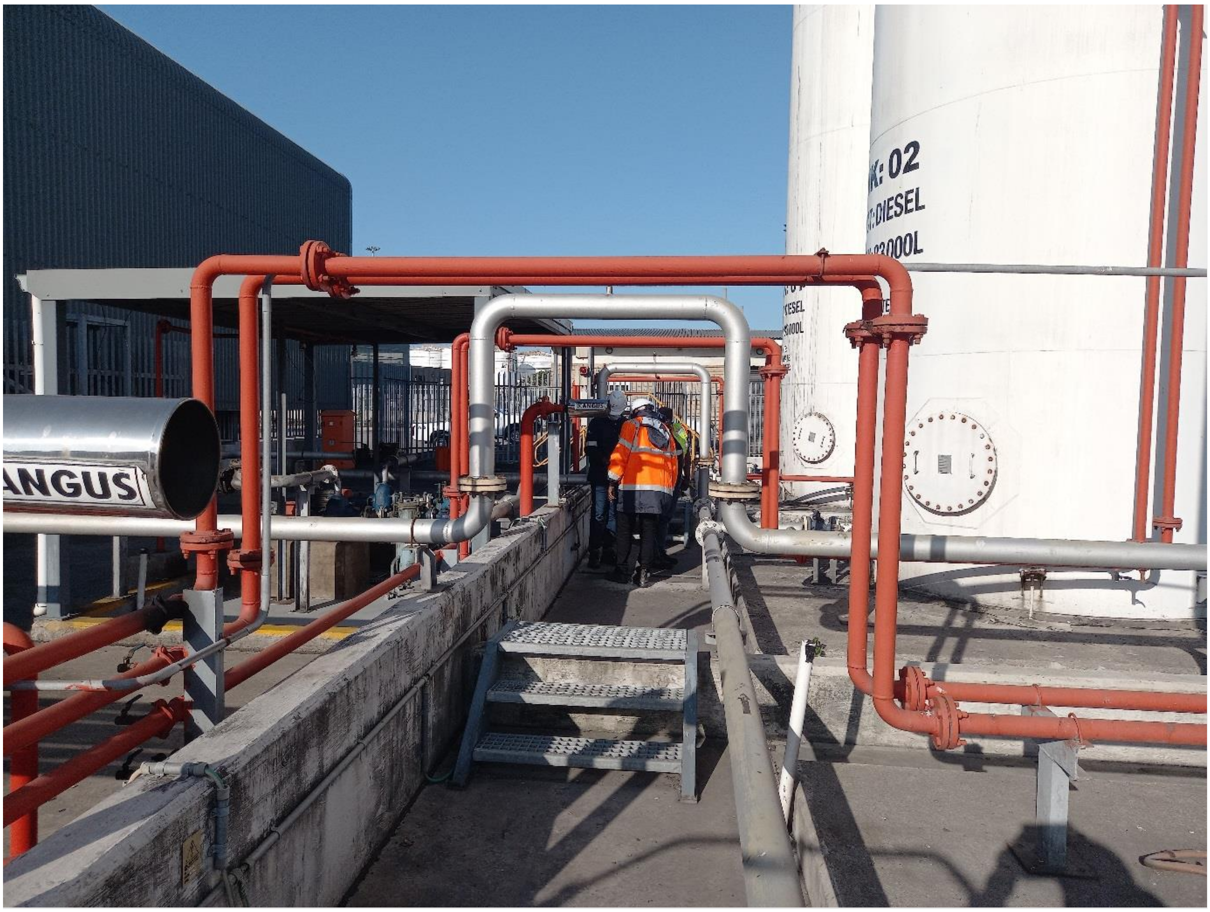
- Annual Ring corrosion protection: Denso wrapping was peeled off and the annular to shell joint is exposed severely to the corrosion. This is the most critical joint of the Tank, which can cause a rupture of a Tank, if corroded severely.
- No overfill protection found.



Annular ring is severely corroded along with piping and valves attached to it

PIPING

- Piping was corroded at various locations.



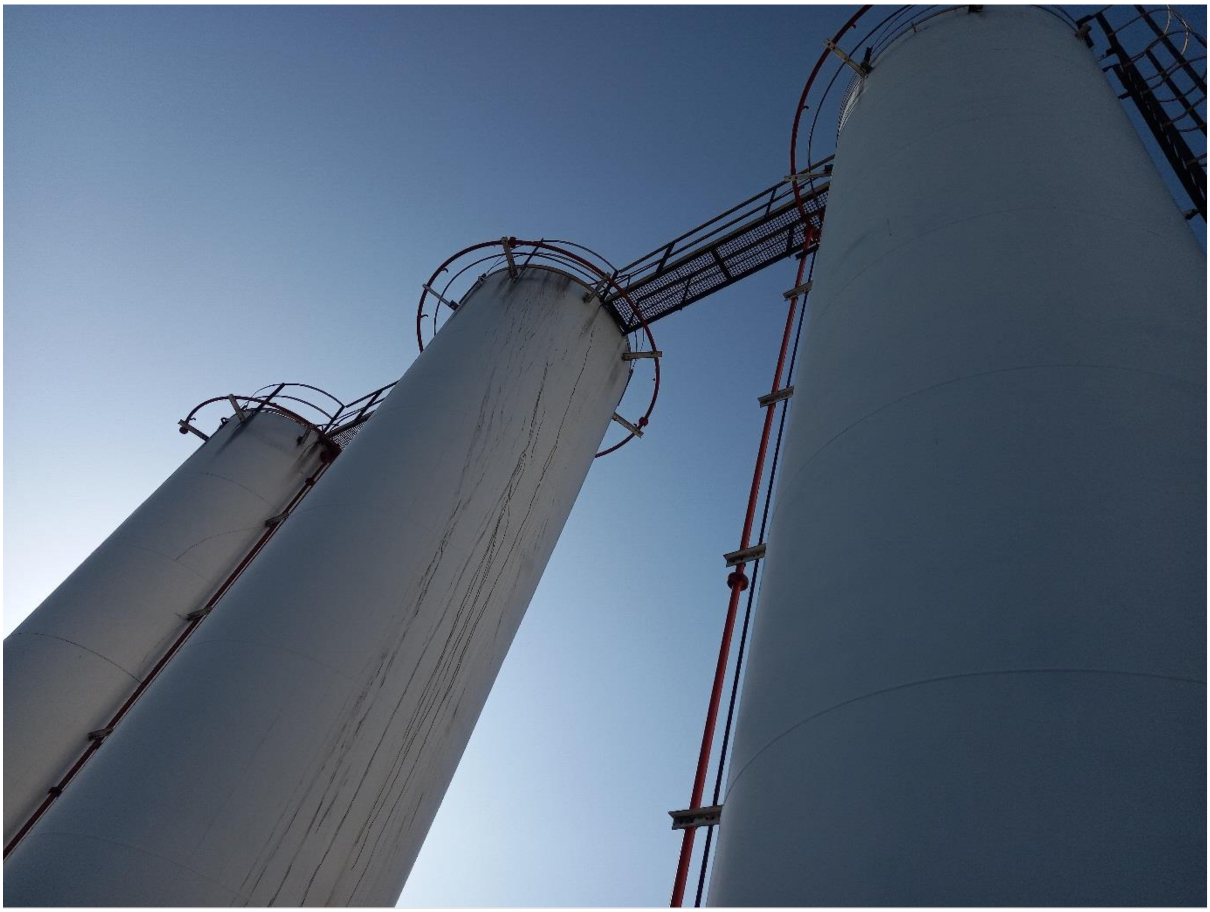
Piping around the Tank and Bunded Area

ELECTRICAL

- Wiring is exposed at several locations.
- Earthing cables are running above ground.

INSTRUMENTATION

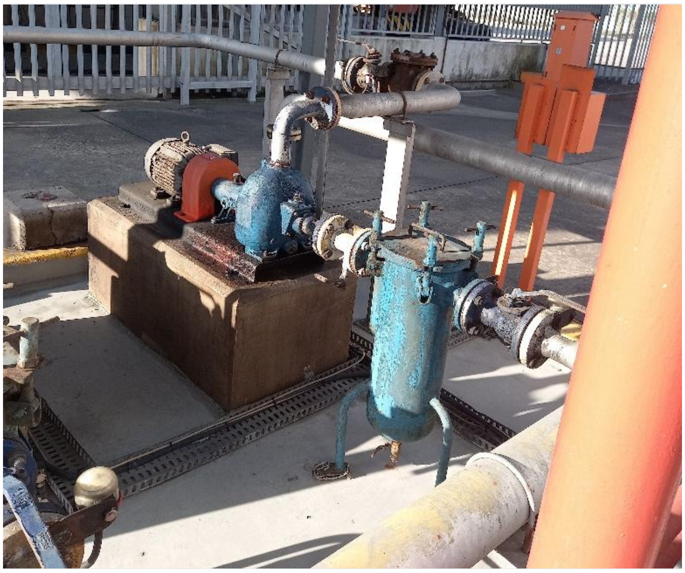
- Instruments needs to be tested.
- Overfill system is not working.



Stain on the Tank indicates that overfill system is not working

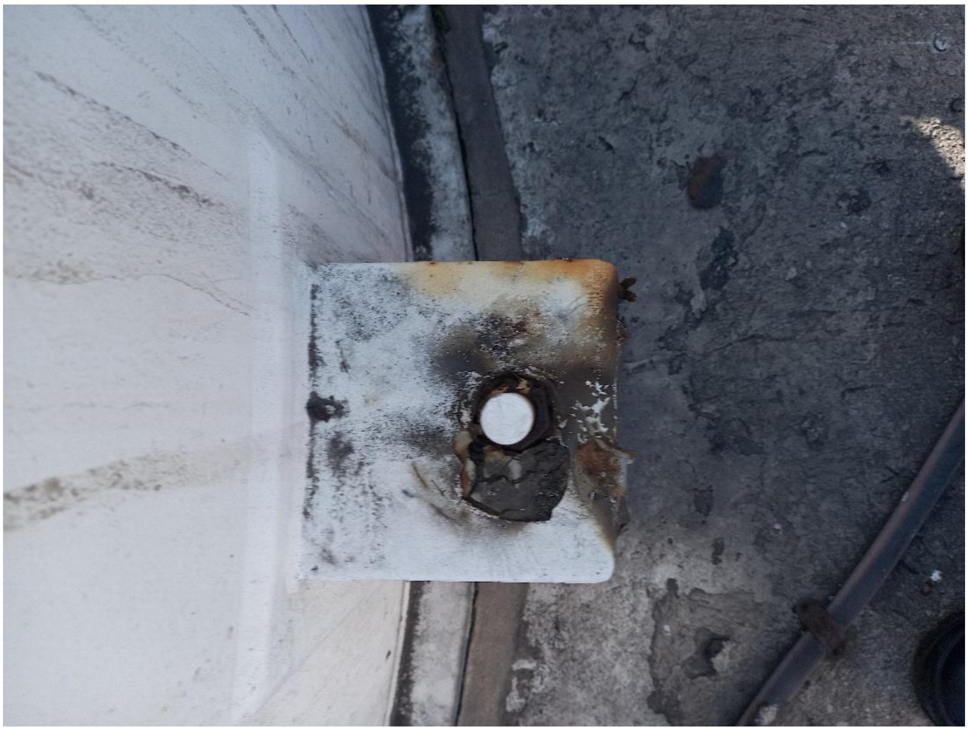
PUMPS

- Maintenance is required on the pumps.



PLATFORMS, LADDERS AND STRUCTURAL

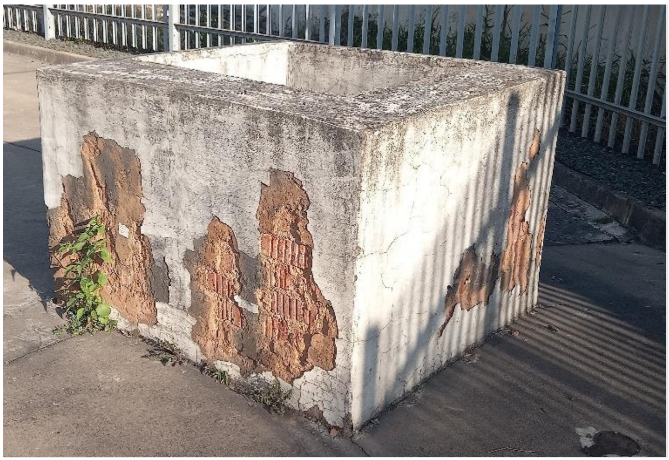
- Corrosion was observed at various locations.
- Top landing attachments are severely corroded and currently it's unsafe to walk on the top platform.



Tank Anchor Chair is severely corroded

CIVIL WORKS

- Tank Anchor chair is severely corroded and may fail if any action is not taken immediately. This will cause overturning moment of the Tank if there are heavy winds.
- Bund walls are cracked.
- Distance from Bund wall to Tank does not comply.
- Sump Tank for water drain needs to be recoated.



Sump Tank to be coated

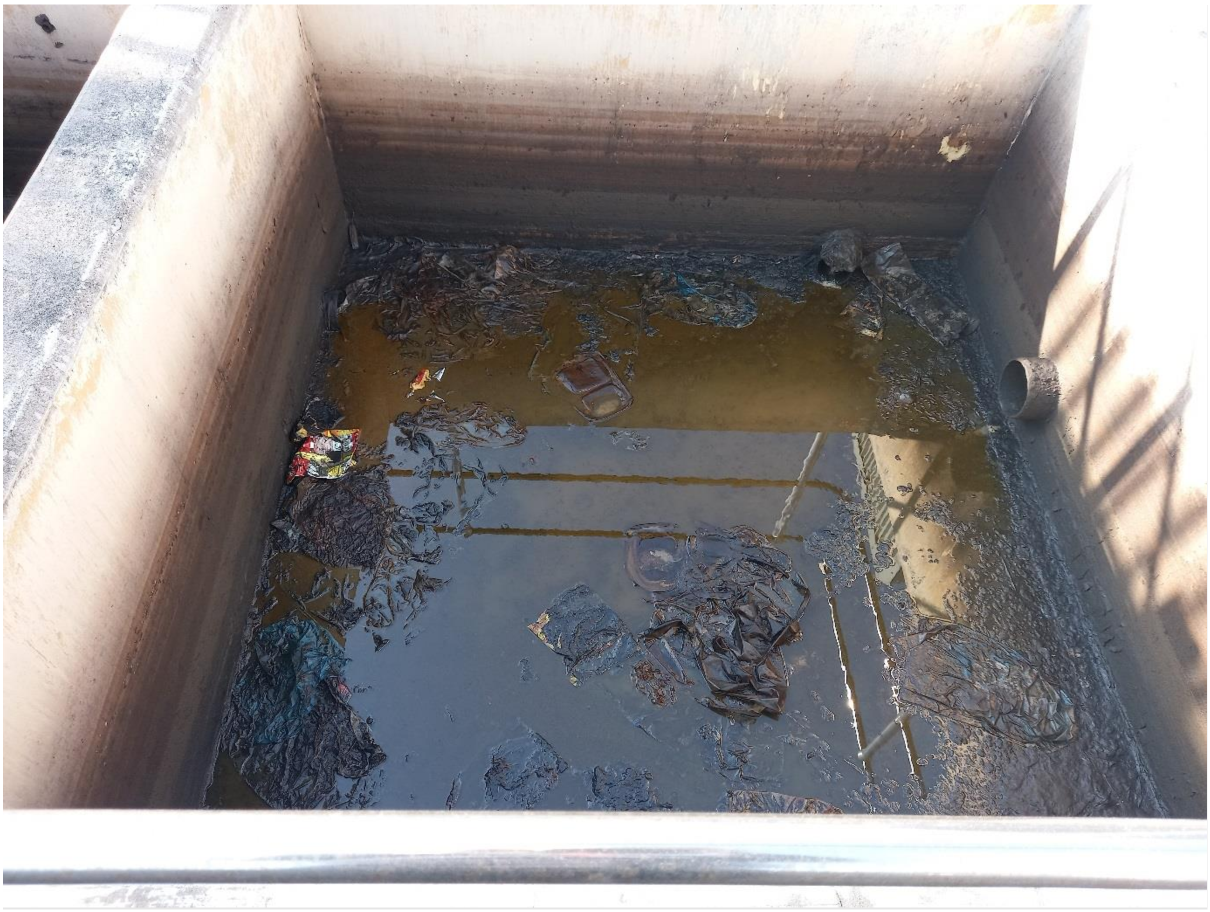


Photo of Oil Water Drain system

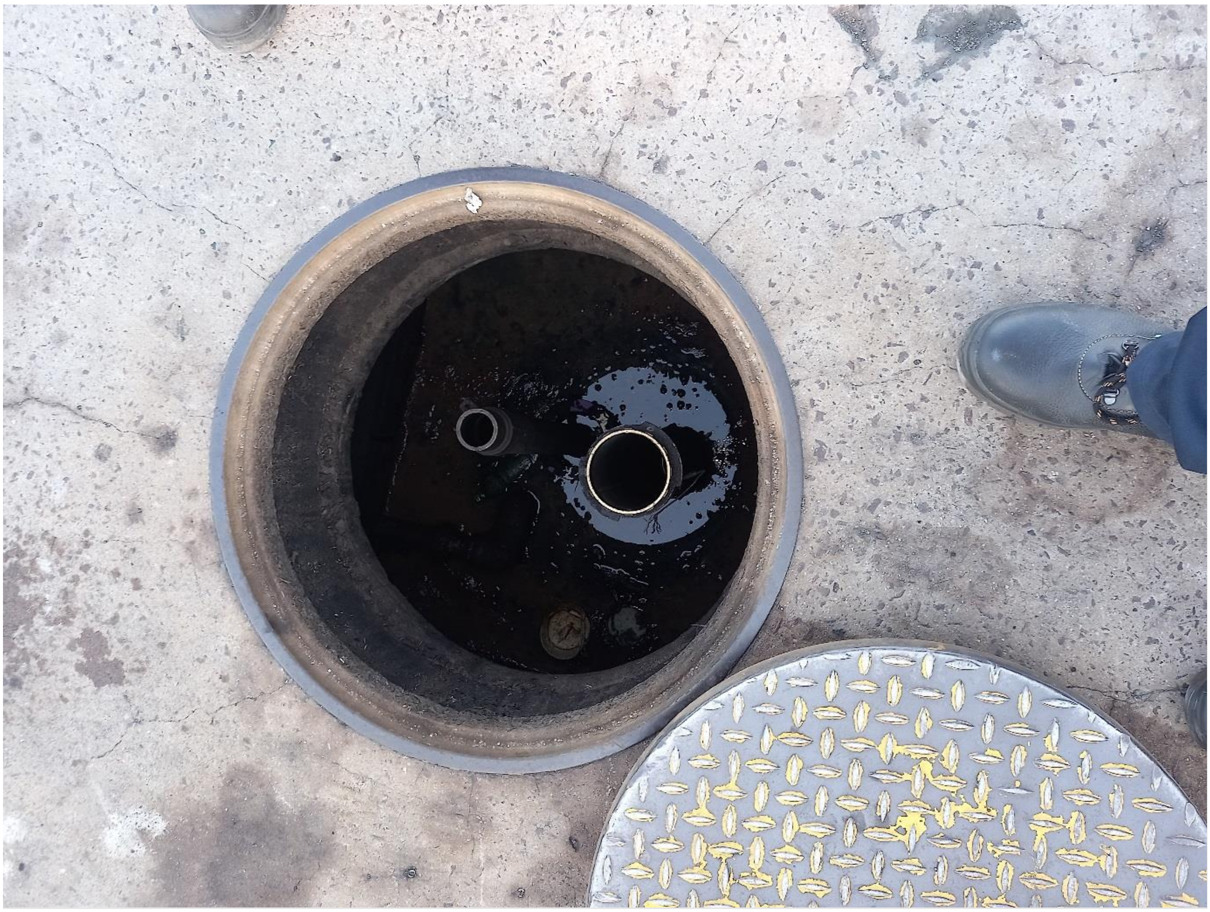
FIRE FIGHTING

- Firefighting system and foam pourers were present on site, but the operators don’t know how to use.

GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Isolation valves don’t have service history.
- No electrical compliance certificates were found.

6.2 DURBAN, PIER 1



The capacity for Pier 1 underground tanks is s x 23 000 L

Phase 2 of expansion, for the new above ground Tanks is immediately applicable for Pier 1, as both the Tanks are below ground. Engineering team has suggested to clean and slurry fill both the Tanks, which is a common engineering practice in the Petrochemical industries, accepted by Environmental authorities not only in South Africa, but globally.

The terminal has identified three locations for new installation, one of the three locations includes one existing location. If the current location is used the terminal will fence the area to improve security.

6.3 RICHARDSBAY

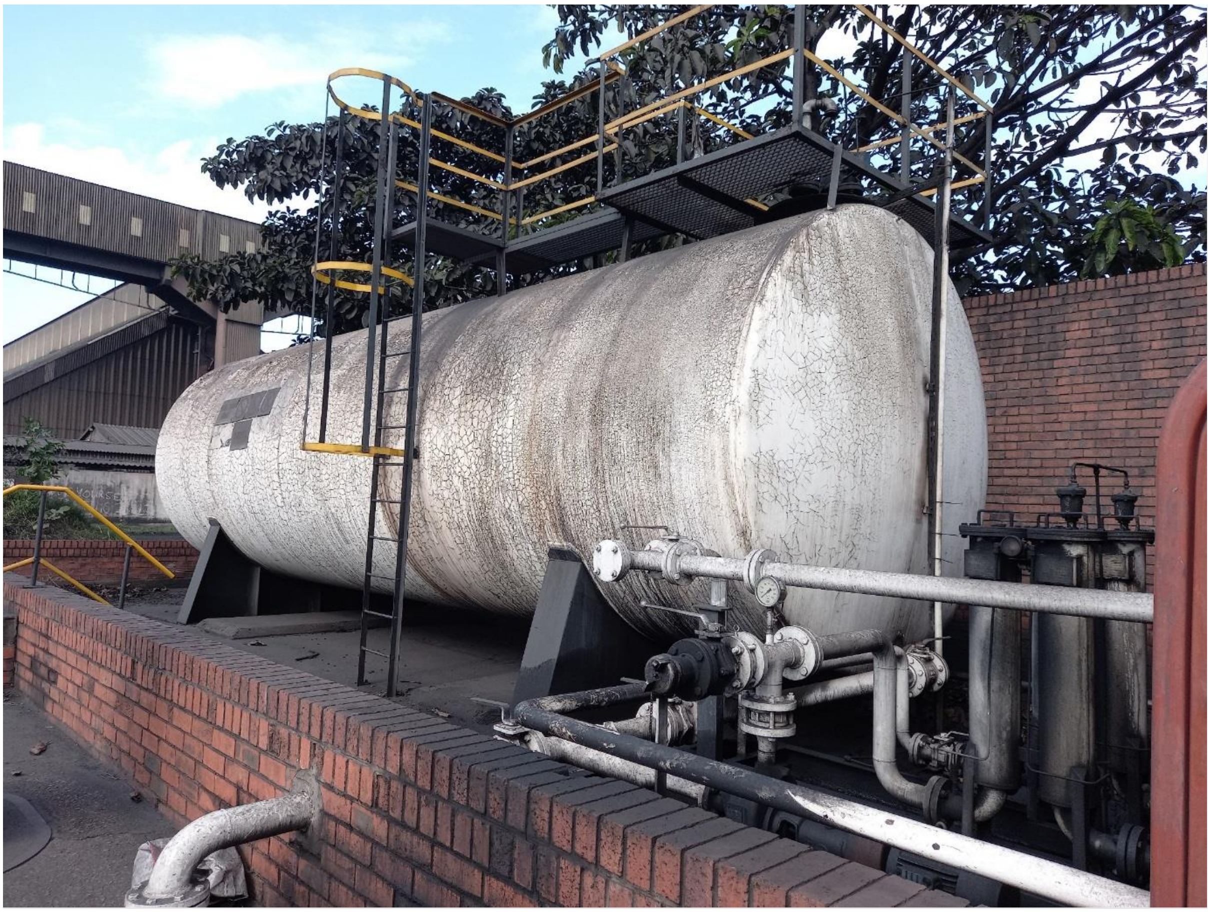


Photo of 60 000 L Diesel Tank

TANKS

- Two horizontal aboveground Tanks were found on site including piping and other accessories, in which one Tank was for Petrol and one for diesel. The petrol Tank was decommissioned and was not in use.
- Diesel capacity was 60 000 L with size 2.9 m diameter and 9 m long.
- Tank is Manufacturer is unknown.
- Paint/ coating is severely cracked and urgently needs to be re-coated.
- Tank was just mounted on the saddles without any welding, which does not comply any code requirement.

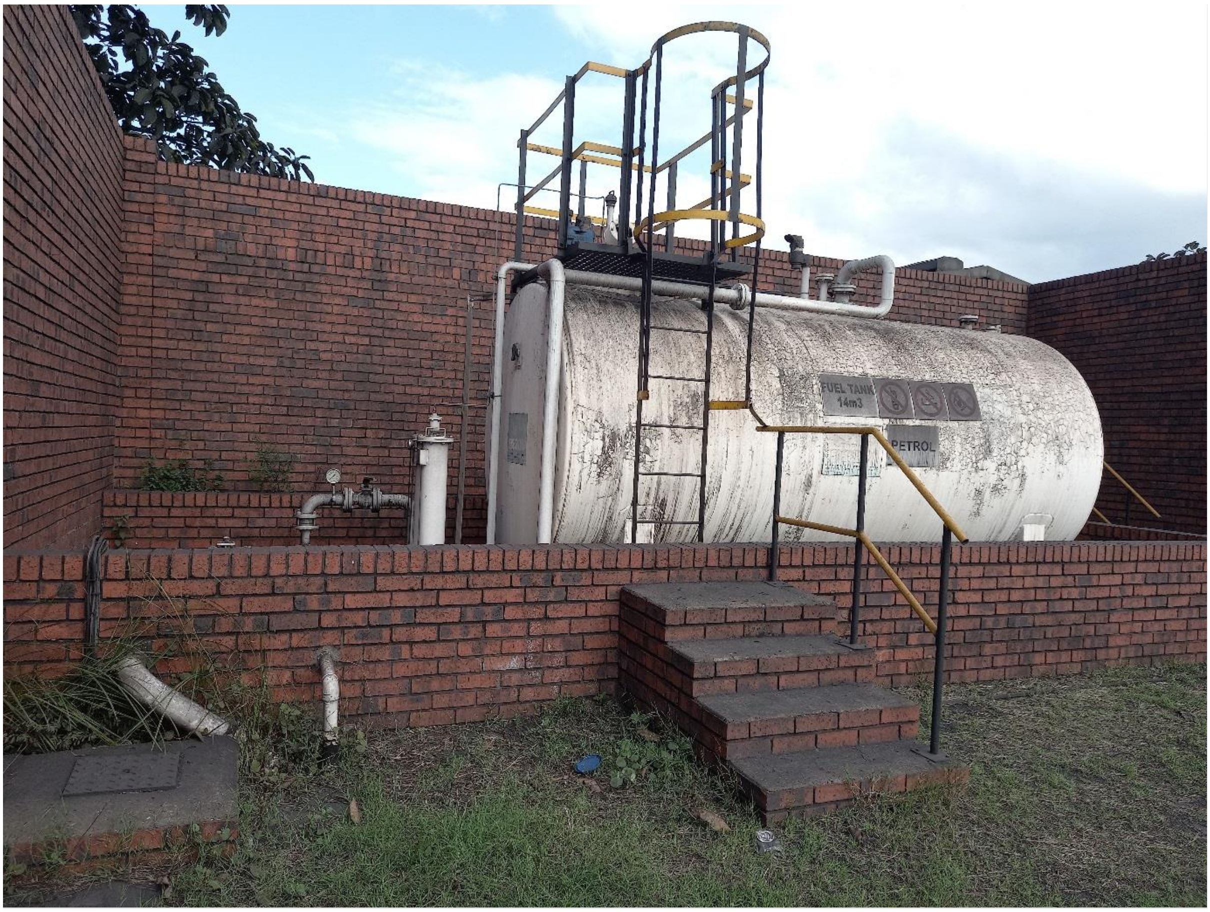


Photo of a Petrol Tank to be demolished along with piping and the bund area

ELECTRICAL

- Wiring is exposed at several locations and DP needs to be reinstalled.
- Earthing cables needs to be organized.

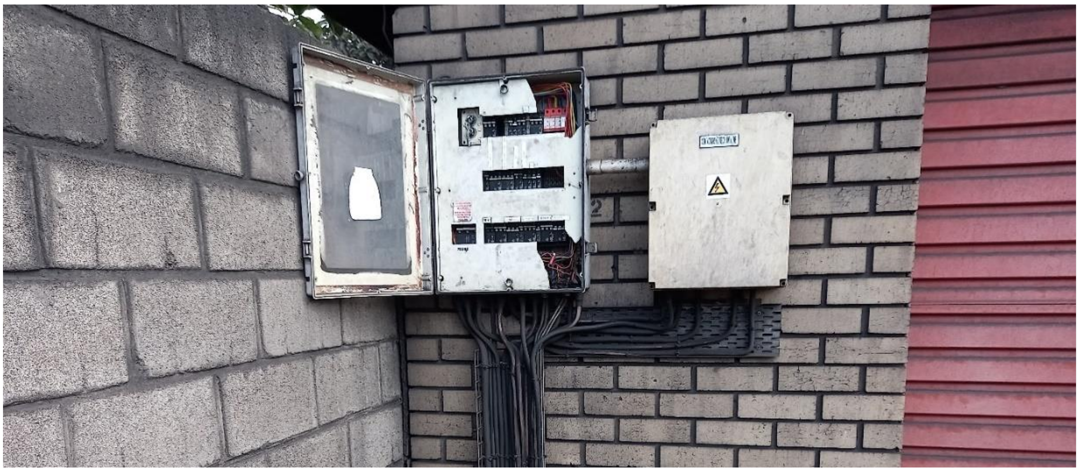


Photo of Electrical cables and the Distribution Board

INSTRUMENTATION

- All Instruments needs to be tested, calibrated, and certified.
- Level indicator/ gauge needs to install.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder and top landing platform need coating at several areas.
- Supports are severely rusted at various locations.

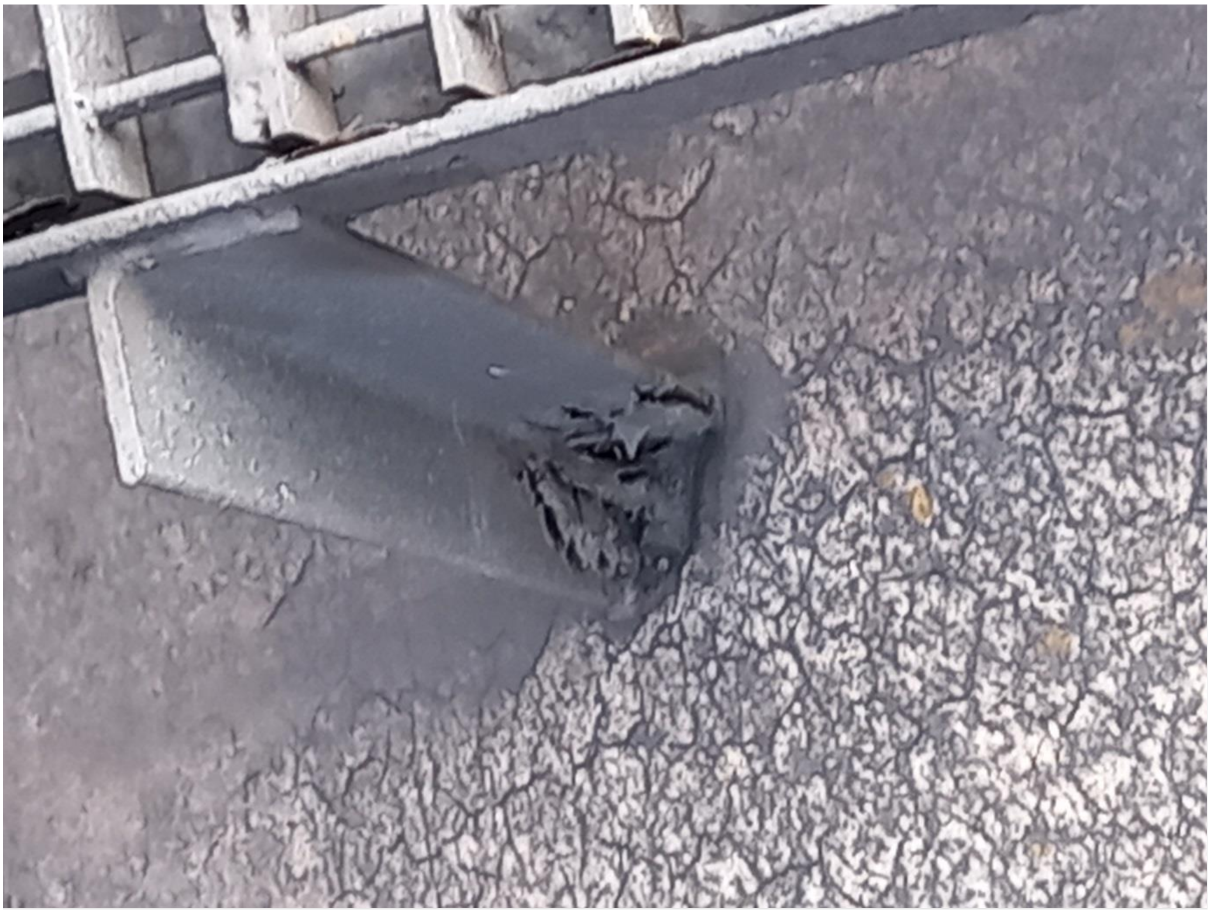


Photo of a rusted support on the Tank for the landing platform

CIVIL WORKS

- Bund walls are cracked.
- Huge tree is growing behind the Bund wall, which may be the root cause of cracking of the bund wall.
- Distance from Bund wall to Tank does not comply
- No arrangements are made for diesel Spillage.

- No arrangements are made for storm water drain.
- Bund area was not clean.
- Vegetation was found around the bunded area.

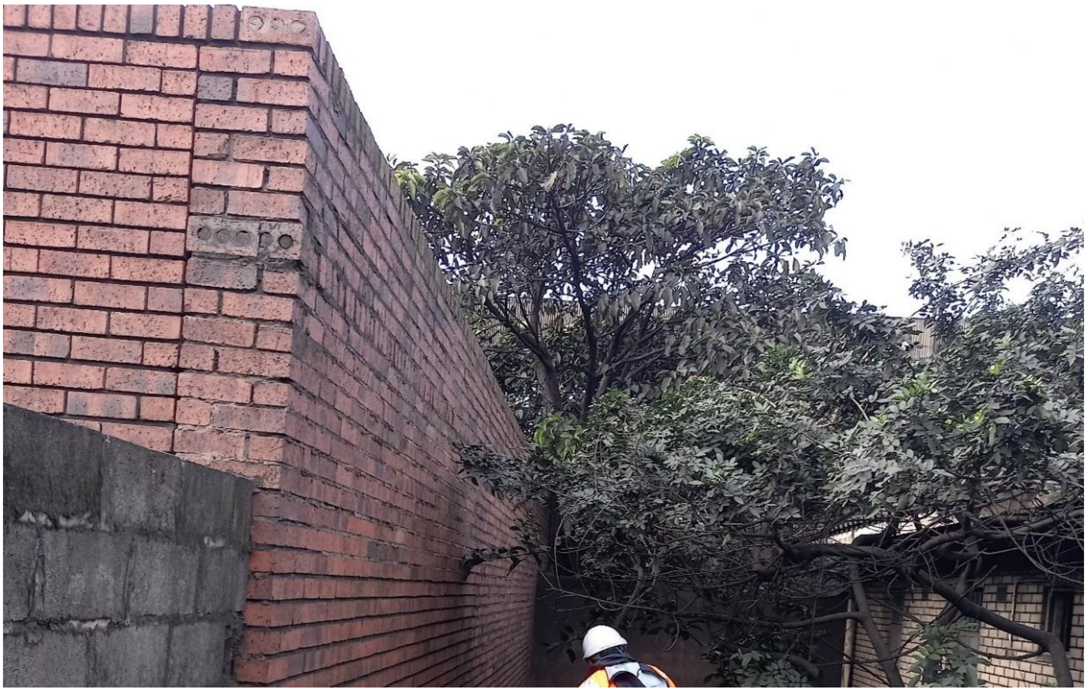


Photo of a tree growing adjustment to the Bund-wall

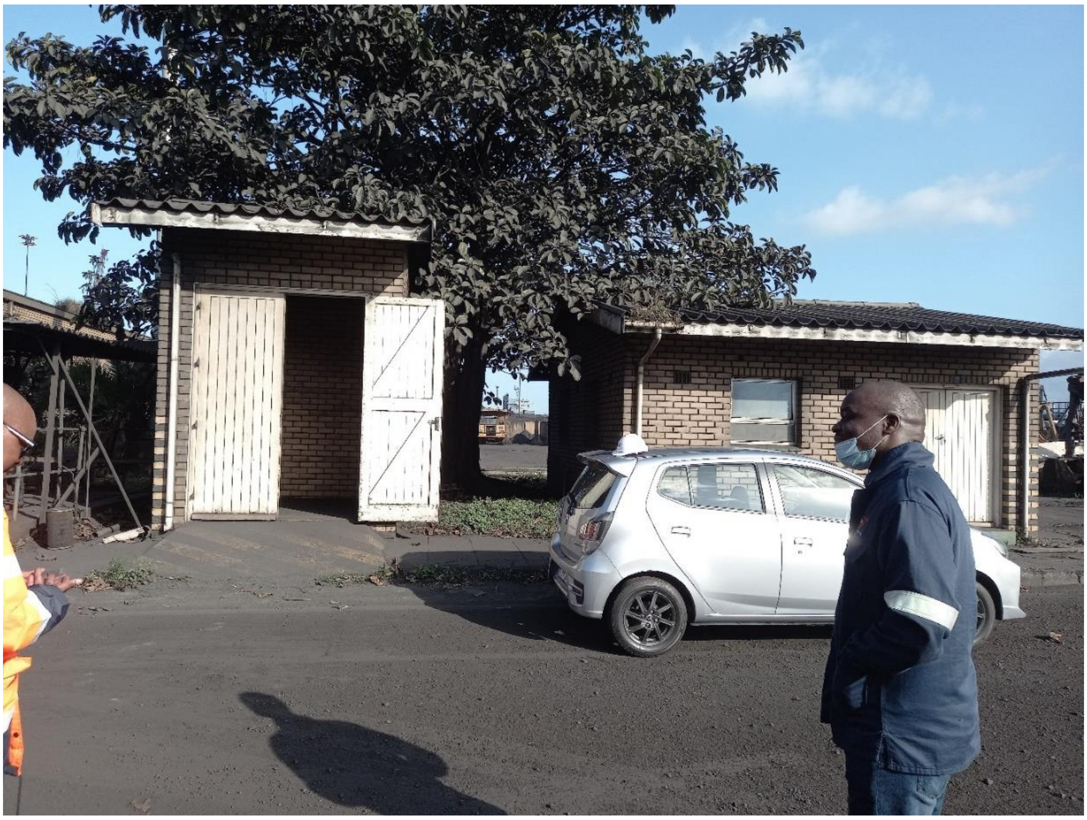
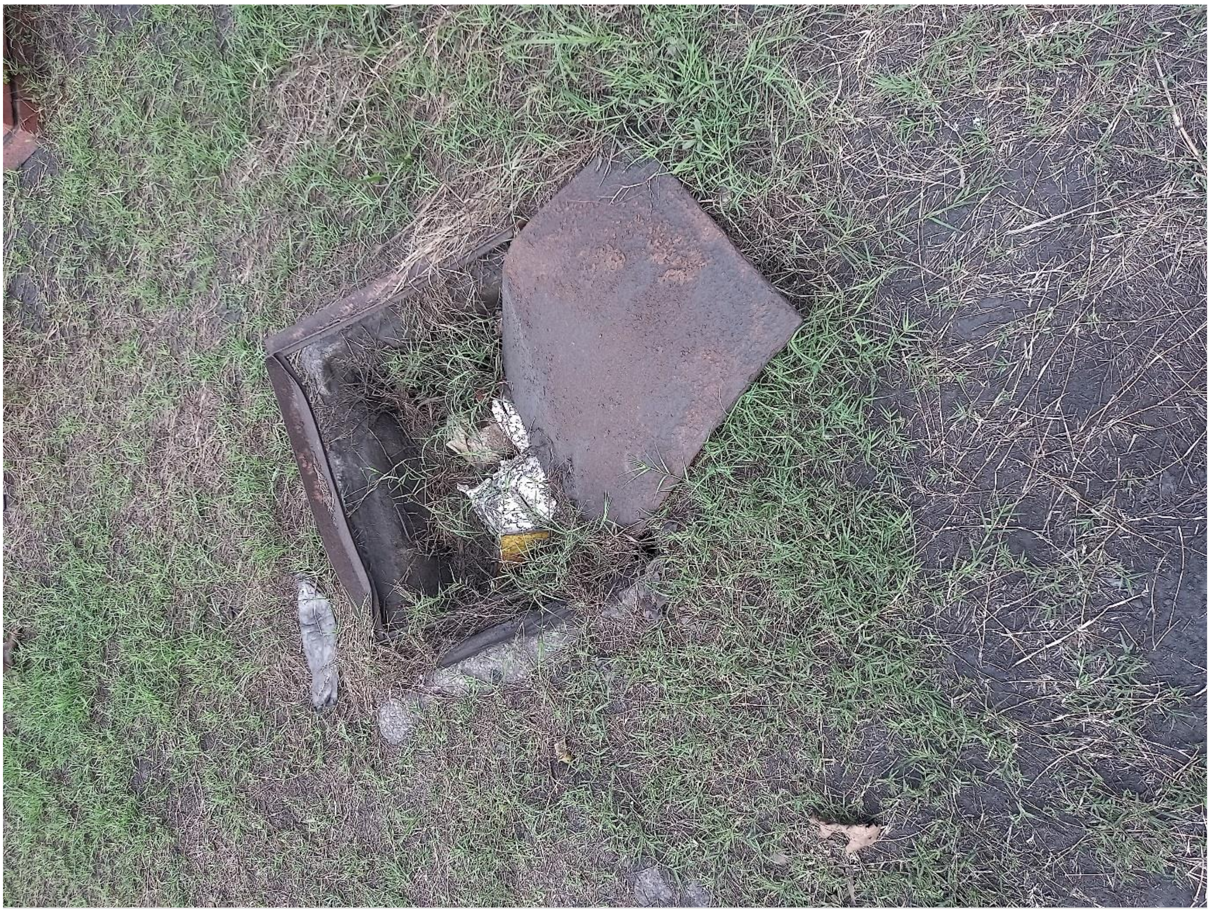


Photo of existing store house and office to demolish



FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

PIPING

- Piping needs to be cleaned and coated.

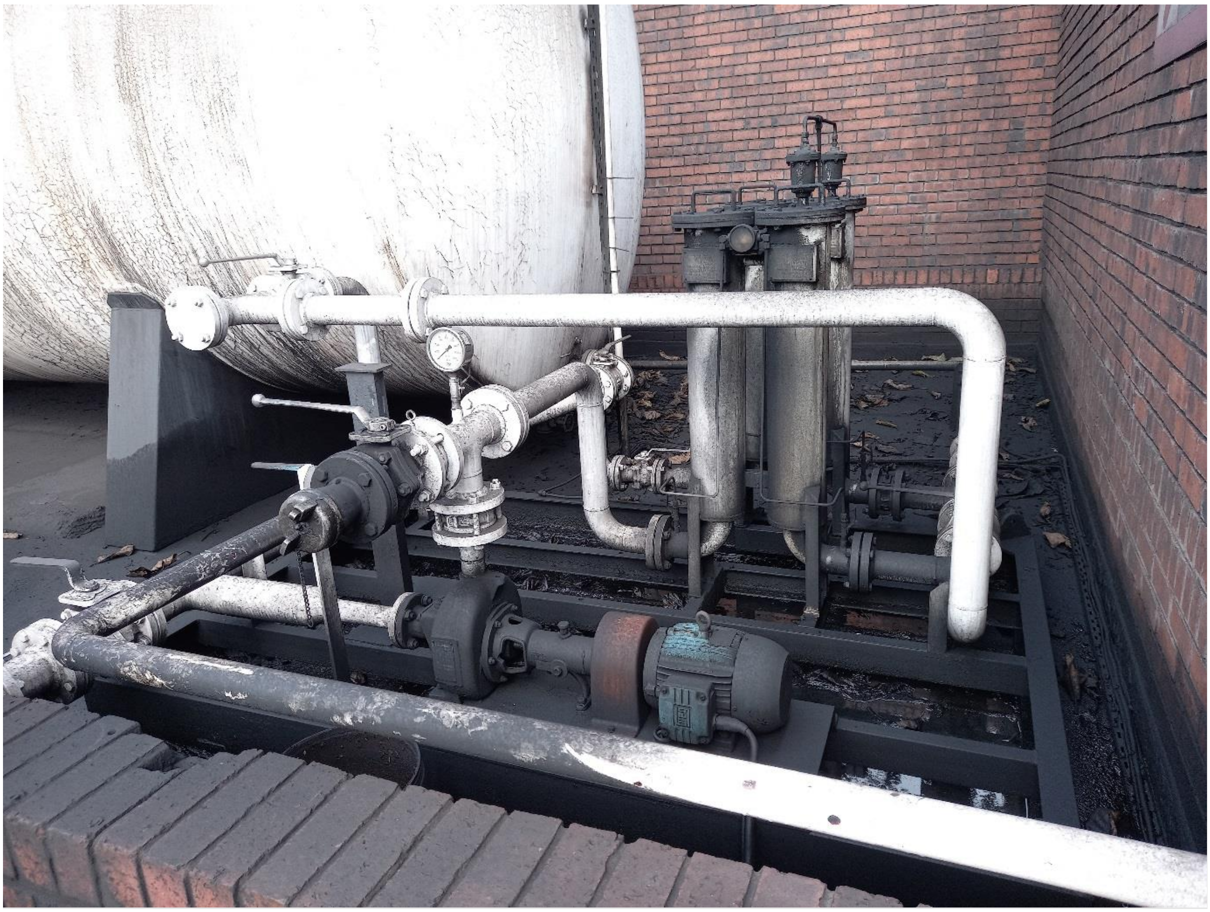


Photo of Piping and Filters

OIL SKIMMER

- Oil Skimmer and underground Oil spillage drain was not in a working condition.
- Cover was rusted severely at some locations.

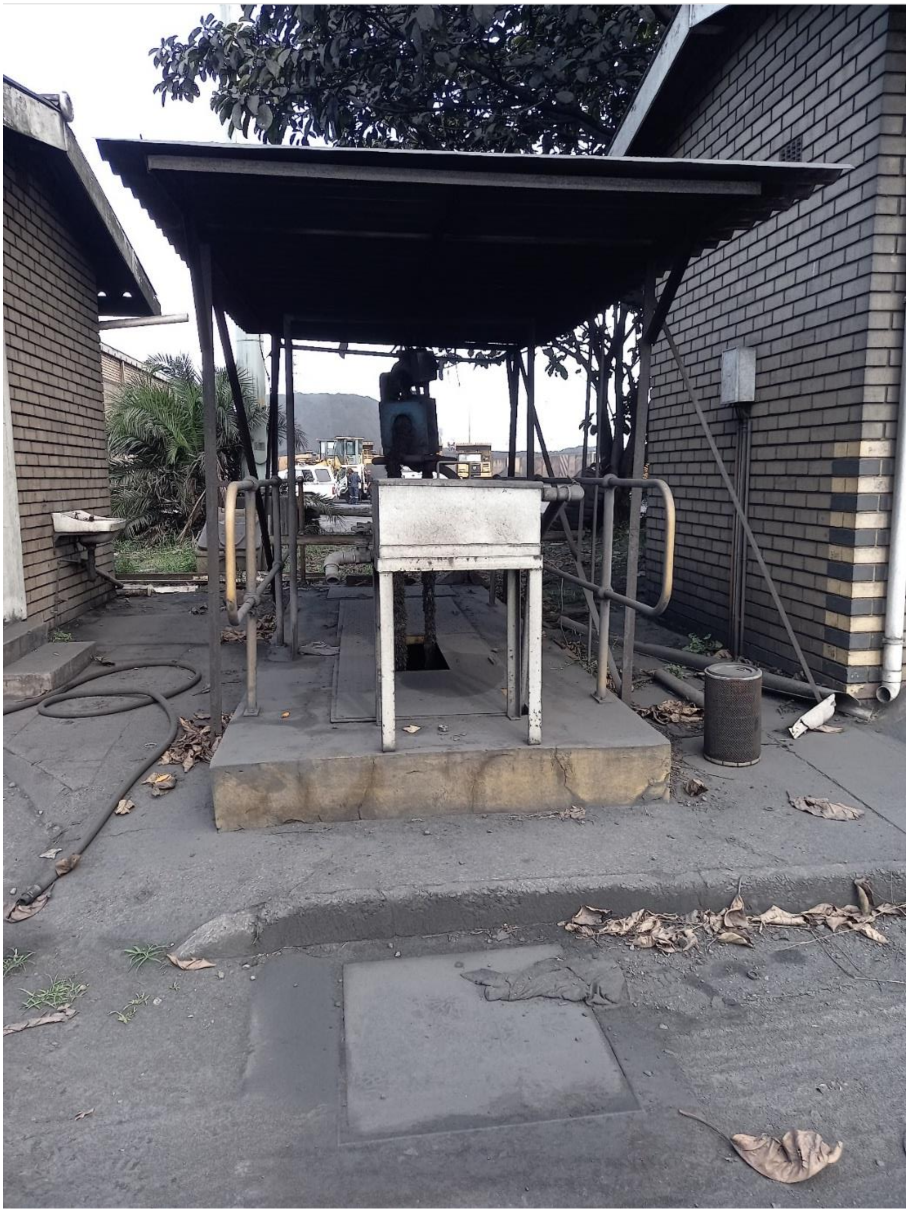


Photo of Oil skimmer

PUMPS

- Maintenance is required on the pumps.

SHADE/ CANOPY

- Existing shade is corroded and is not in a good condition.
- Site team, operating these tanks has requested a big new canopy.

Photo of an existing canopy

GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.

PHASE 2

- Three locations are proposed for Phase Two, which includes one existing location.

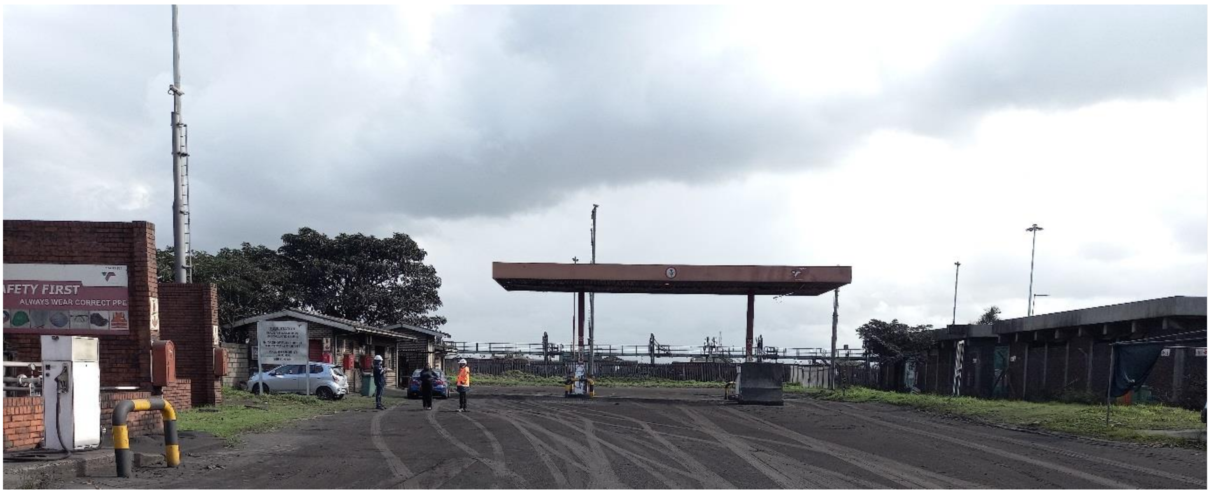


Photo of Phase two: option one: Existing Area

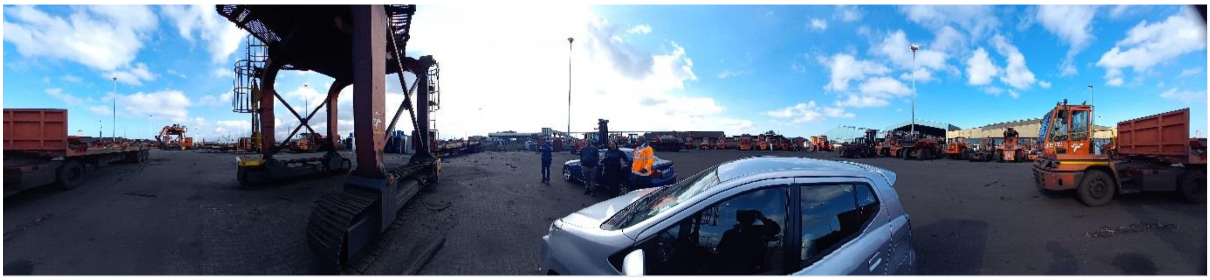


Photo of Phase two: option two:

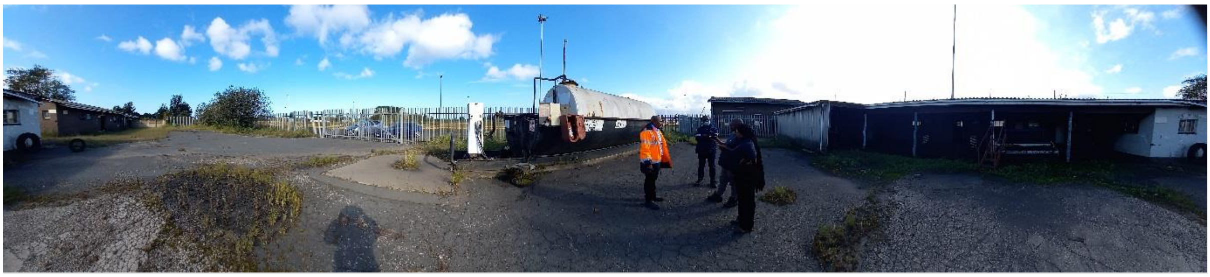


Photo of Phase two: option three:

6.4 POINT TERMINAL, MPT

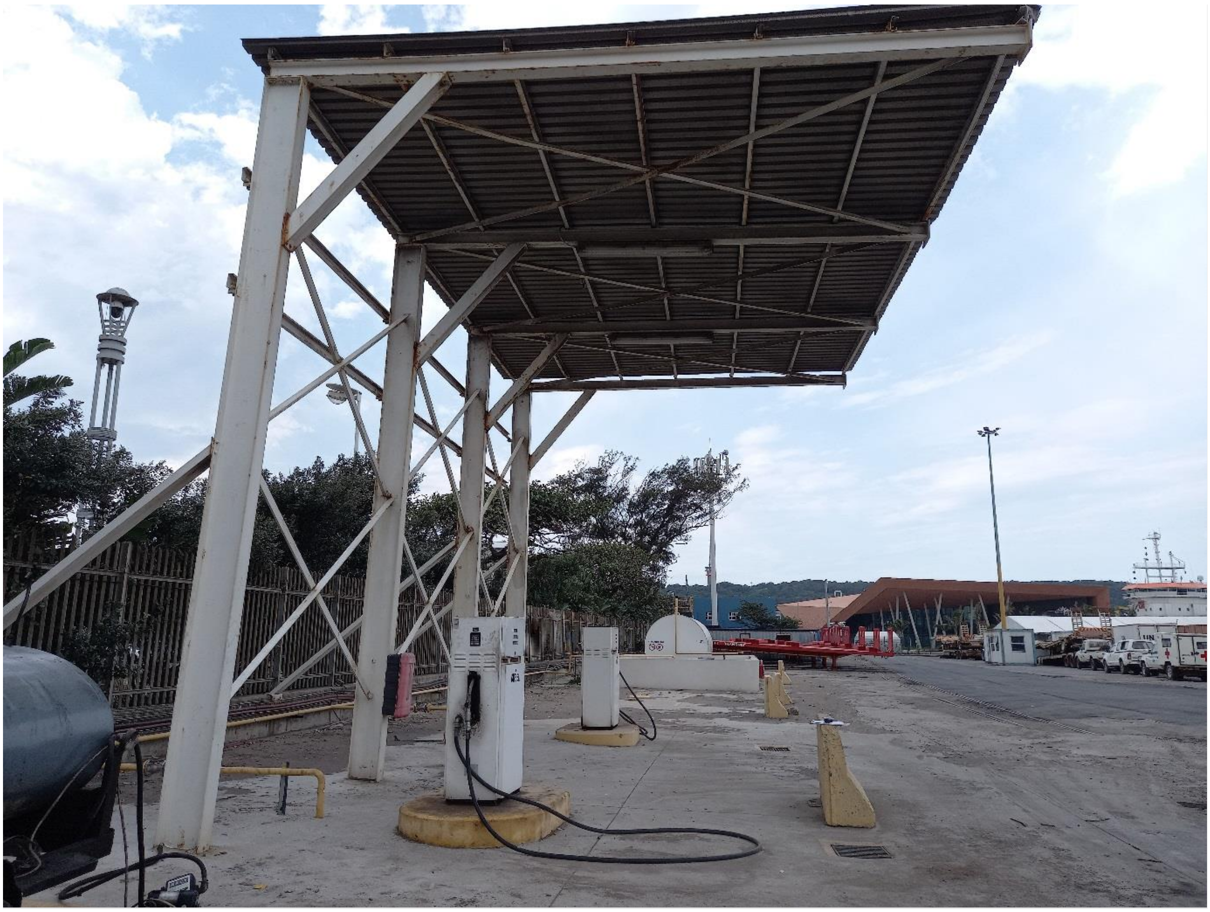


Photo of Point Road Diesel Tank and dispensers

TANKS

- One horizontal aboveground Diesel Tanks was visually inspected on site including piping and other accessories.
- Tank is mounted on the structural support.
- Diesel capacity was 23 000 L with size 2.4 m diameter and 5.52 m long.
- Paint/ coating is in an average condition.

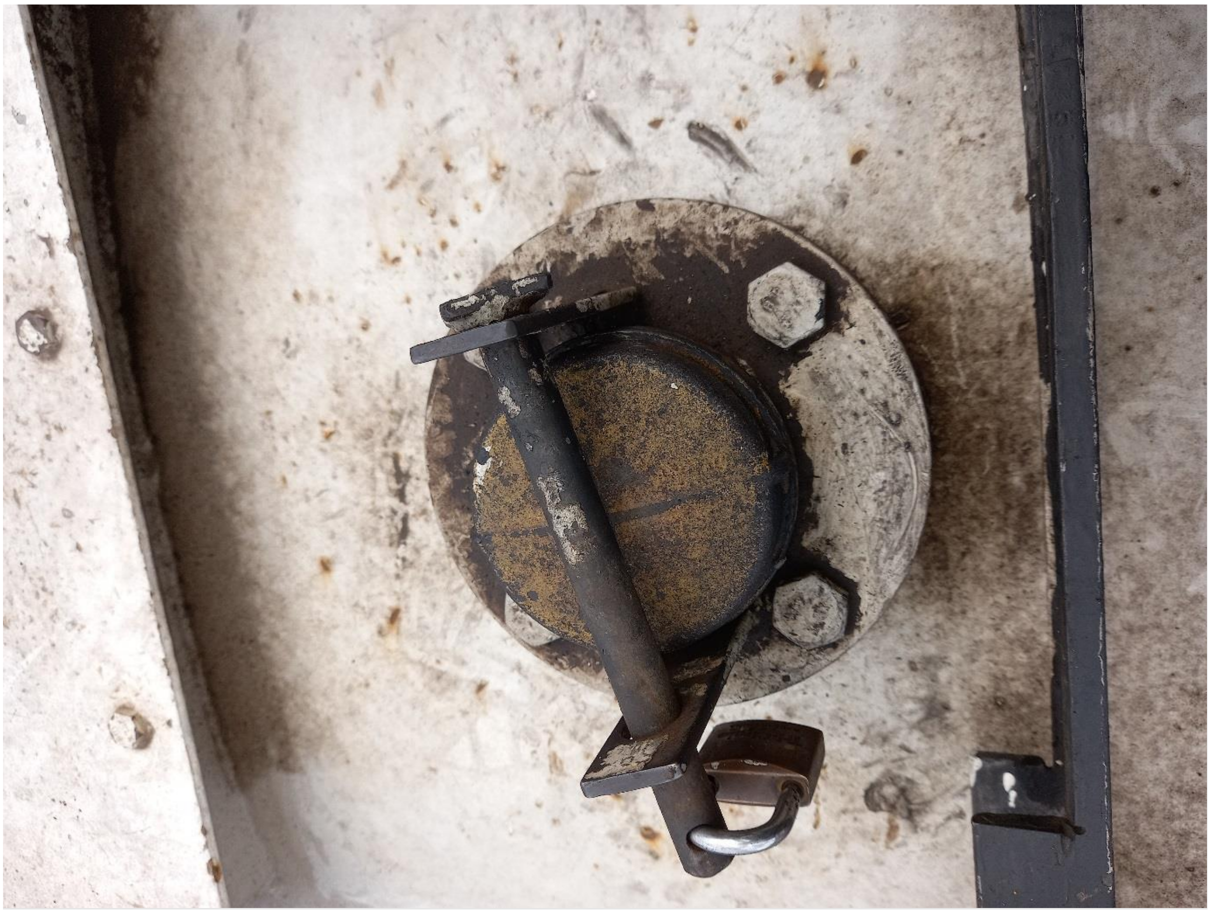


Photo of a coating peeling off on the rectangular manway

ELECTRICAL

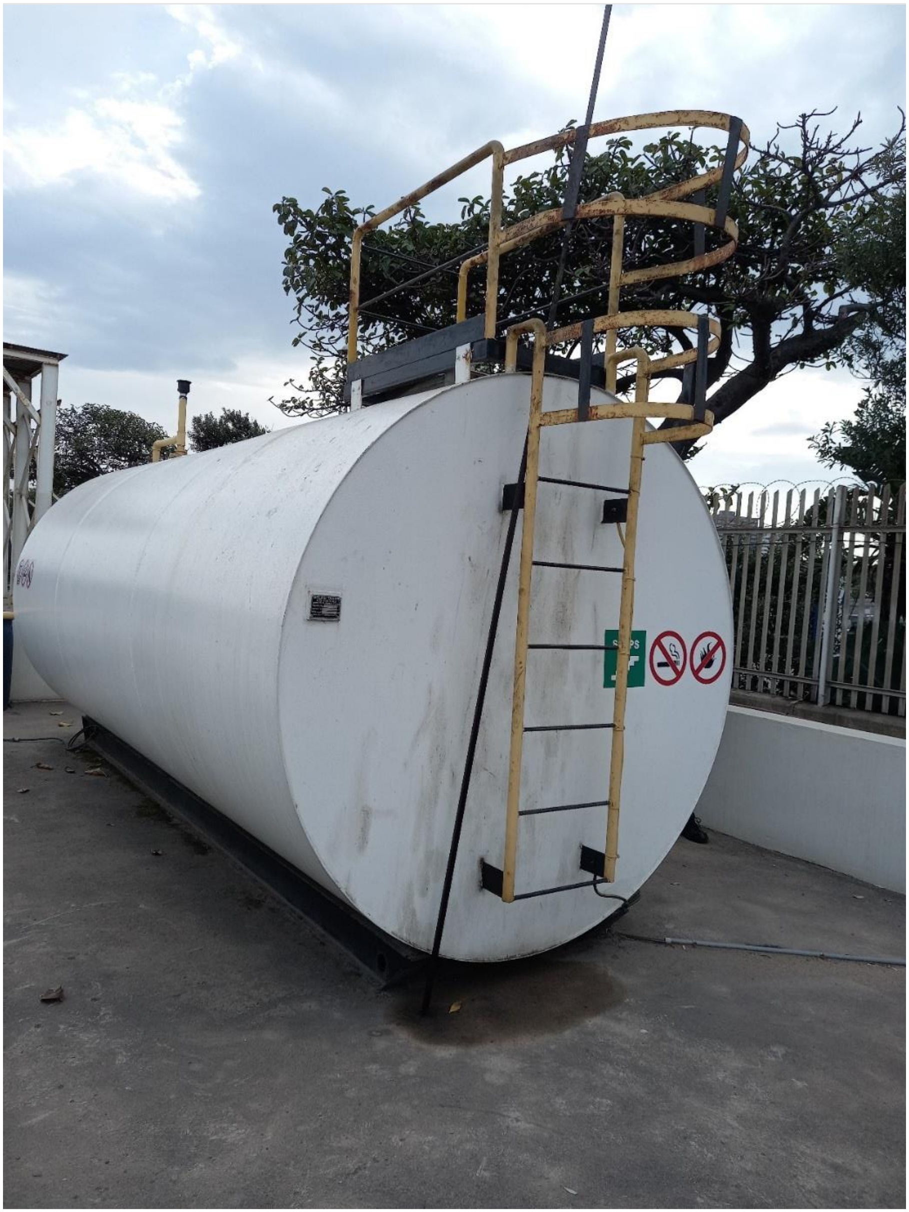
- Wiring and DP was in a good condition.
- Earthing cables needs to be organized.

INSTRUMENTATION

- All Instruments needs to be tested, calibrated, and certified.
- Level indicator/ gauge needs to be installed.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder and top landing platform need coating at several areas.
- Stairs and railing to enter the bund area are intact and in a good condition.



Platform, ladder etc. are rusted

CIVIL WORKS

- Bund walls are in a good condition.
- Bund size: 10.54 m long x 5.8 m wide x 840 mm height.
- Bund area was not clean.
- Vegetation was found around the bunded area.

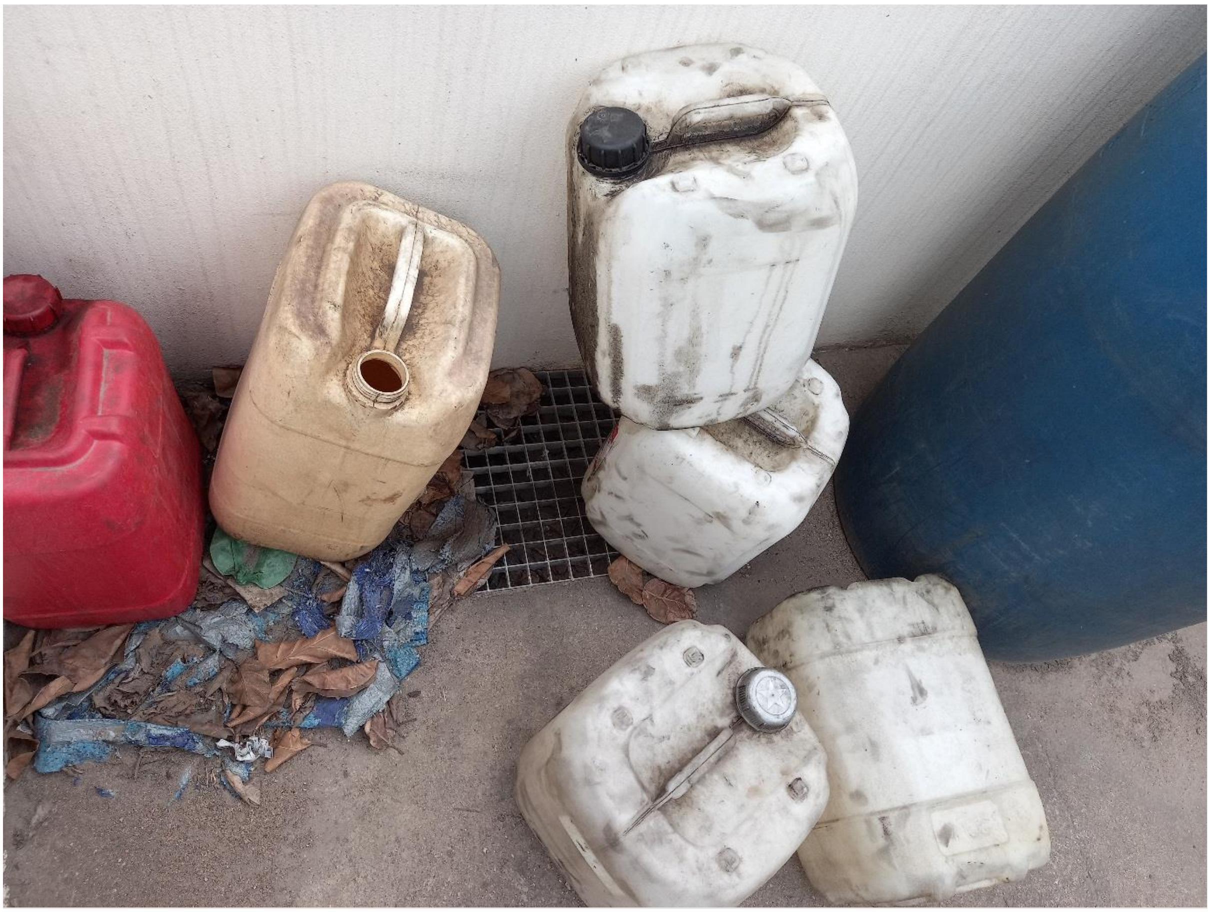


Photo of a Storm water / Diesel Spillage drain

FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

OIL SKIMMER

- Oil Skimmer and underground Oil spillage drain was not found.

PUMPS

- Maintenance is required on the pumps.

SHADE/ CANOPY

- Site team, operating these tanks has requested a big new shade.

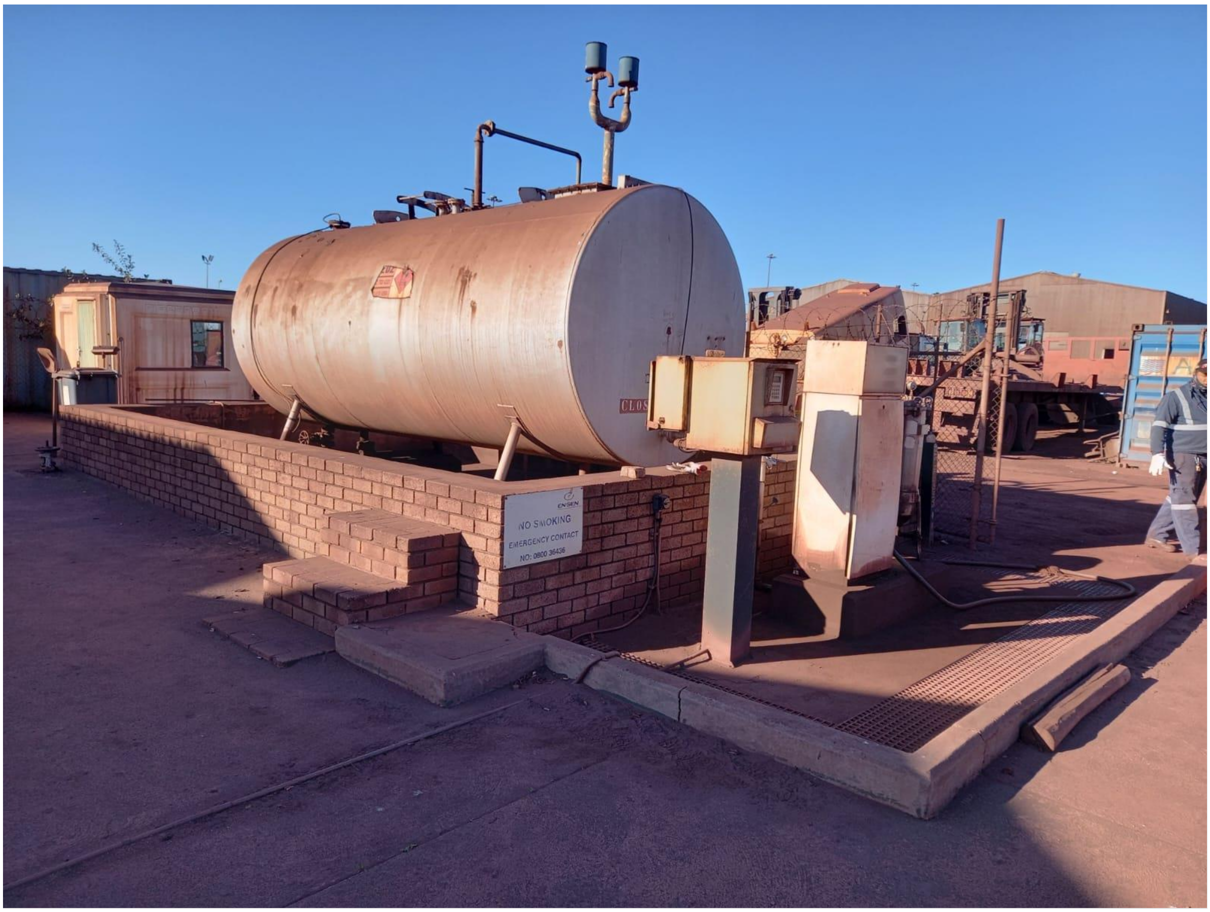
GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.

- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.

PHASE 2

6.5 SALDHANA



23 000 L Tank: Diameter 2.3 m x 5.4 m Long Bund-wall

TANKS

- One horizontal aboveground Diesel Tanks was visually inspected on site including piping and other accessories.
- Tank is mounted on the structural support.
- Diesel capacity was 23 000 L with size 2.4 m diameter and 5.4 m long.
- Tank Manufacturer: No nameplate found
- Paint/ coating was in a worst condition. Tank is constantly under various chemical attack, which are loaded/unloaded in the port with the recent addition of manganese. Big Lumps are formed due to the heavy corrosion.
- Nozzles are severely corroded.

ELECTRICAL

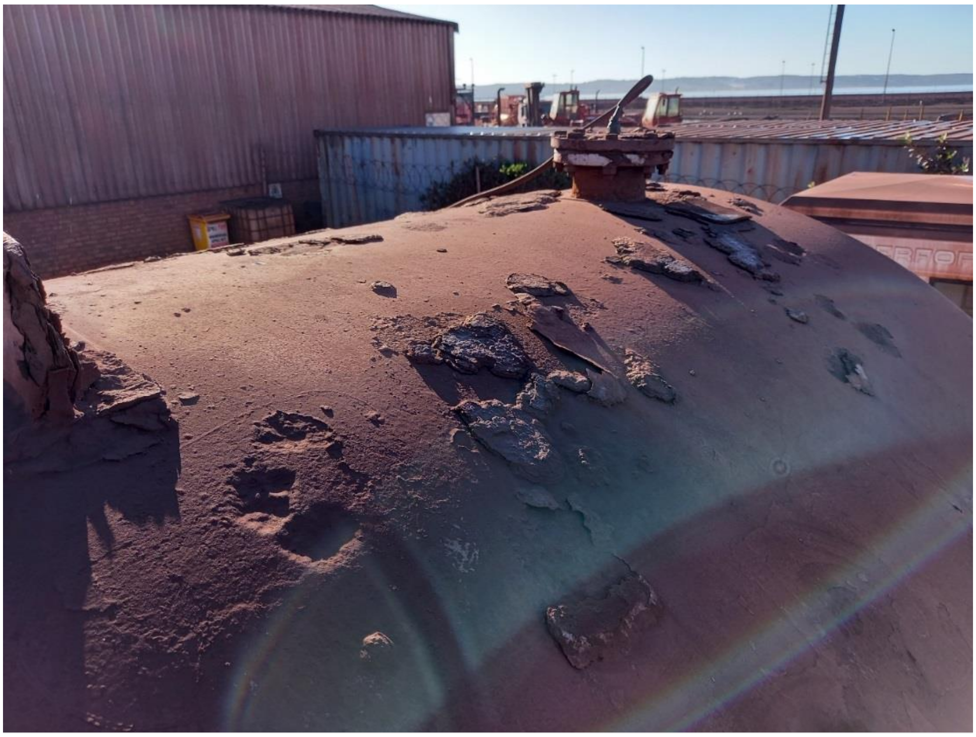
- Wiring and DP was in a good condition. but was installed in a canteen, far away from the facility.
- Earthing cables needs to be organized.

INSTRUMENTATION

- All Instruments needs to be tested, calibrated, and certified.
- Level indicator/ gauge needs to install.
- Breathers need to be tested.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder needs complete coating.
- No top landing platform was identified.
- No walkway or landing platform was installed.
- Saddle/support was not welded to the Tank.



CIVIL WORKS

- Bund walls are in a good condition.
- Bund size: 6.9 m long x 4.6 m wide x 330 mm height.
- Bund area was not clean.
- Vegetation was found around the bunded area.
- Drain was blocked.

FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

OIL SKIMMER

- Oil Skimmer and underground Oil spillage drain was not found.

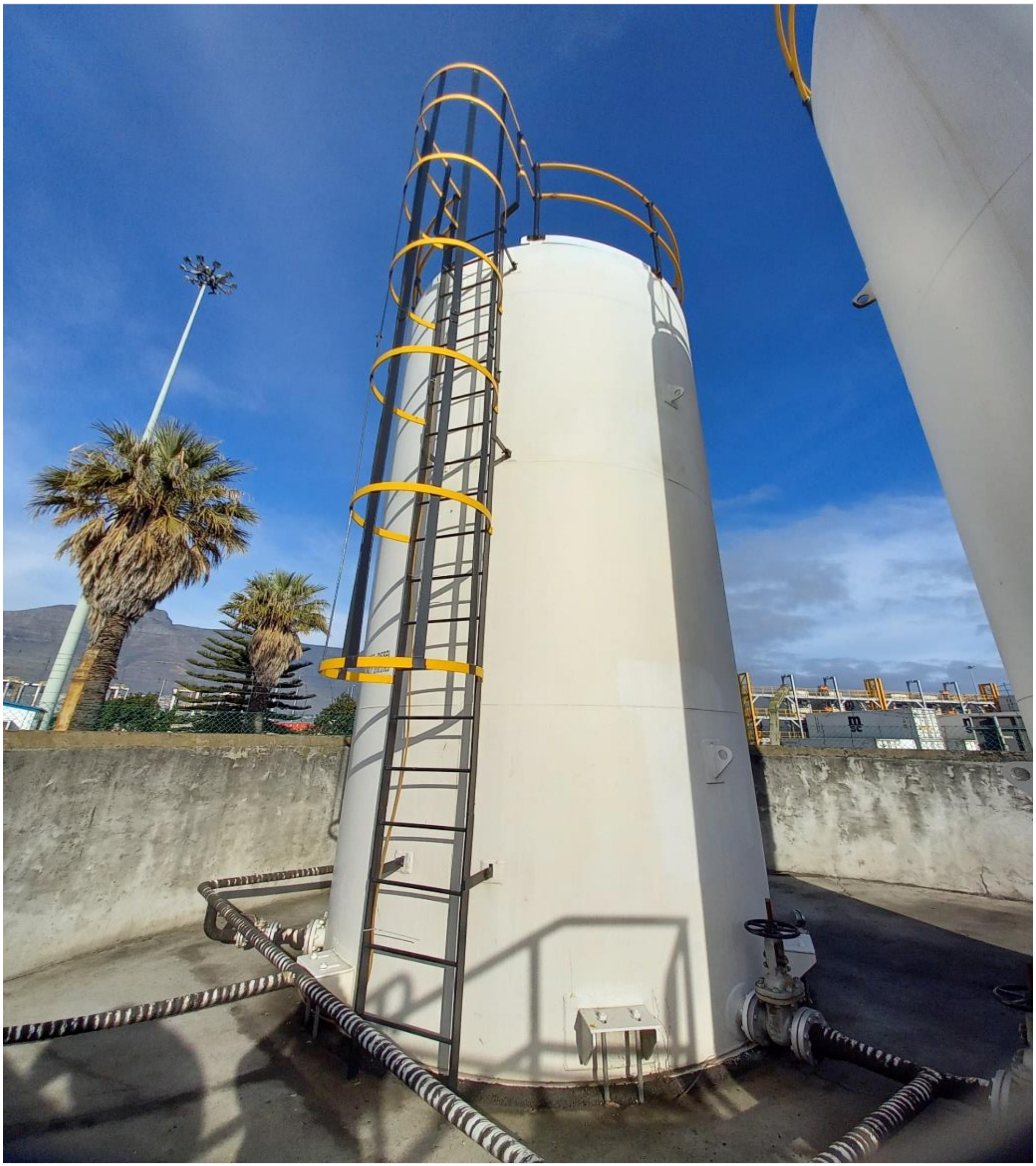
PUMPS

- Maintenance is required on the pumps.

GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Tank needs to be washed/ rinsed everyday due to excessive corroded condition.

6.6 CAPE TOWN



2 x 39000 L Tank: Diameter 2.82 m x 6 m Long

TANKS

- Two Vertical Aboveground Diesel Tanks were visually inspected on site including piping and other accessories.
- Tank is mounted on the annular ring which had a Denso wrapping.
- Each tank has Diesel capacity 39 000 L with size 2.82 m diameter and 6 m height.
- Tank Manufacturer: Tseba Construction (PTY) LTD.

- Paint/ coating was in a bad condition at multiple locations.
- Top Nozzles are severely corroded.
- Corrosion was spotted at various locations.
- Flange/ bolt sizes were different and incorrect at some places.
- Anchor chair bolts were bent.
- MHI is required.

ELECTRICAL

- Wiring and DP was in a good condition.
- Earthing cables needs to be organized.

INSTRUMENTATION

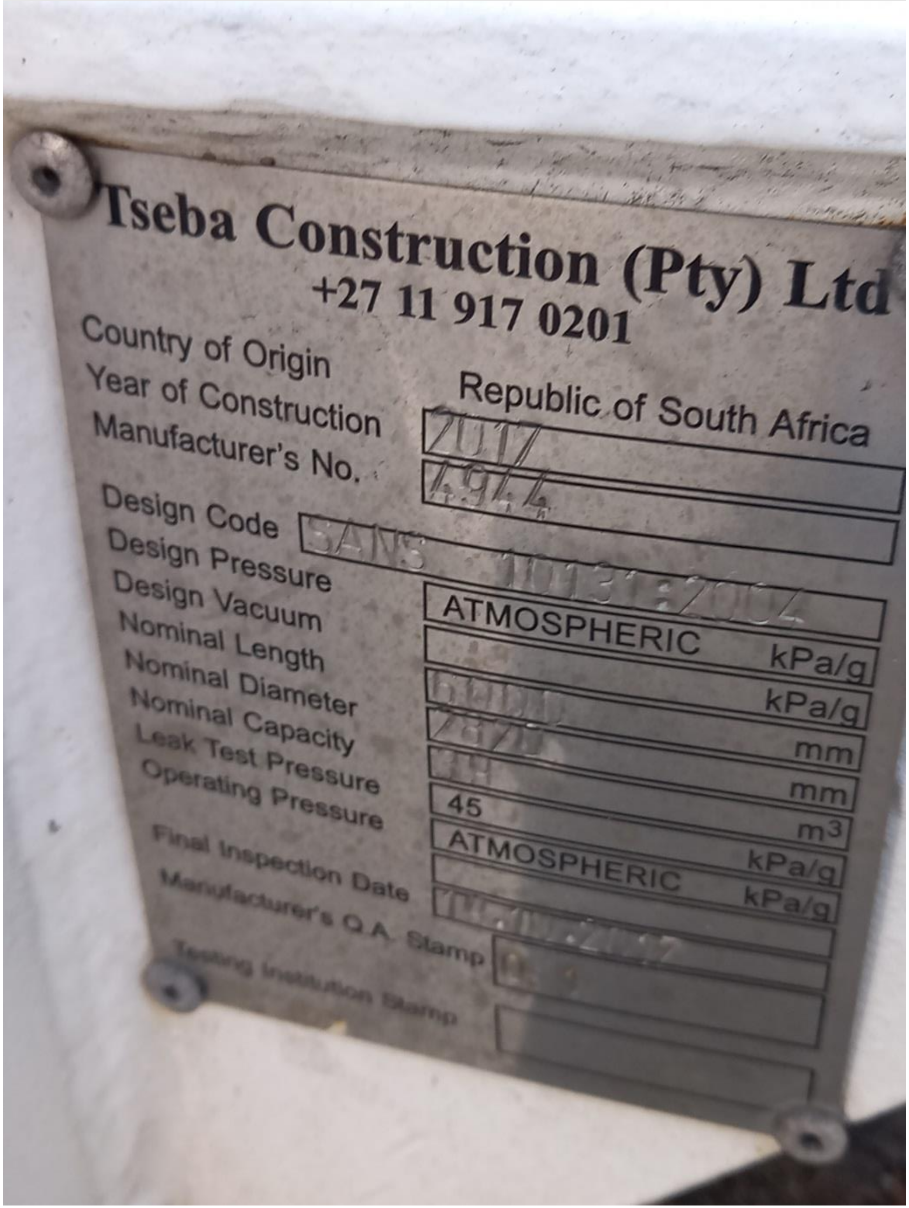
- All Instruments needs to be tested, calibrated, and certified.
- Level indicator/ gauge needs to install.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder needs complete coating.
- No top landing platform was identified.

CIVIL WORKS

- Bund walls are in a good condition.
- Bund size: round bund-wall with 900 mm (worst distance)
- Bund area was clean.
- Vegetation was found around the bunded area.
- Drain was not identified.



Tseba Construction (Pty) Ltd
+27 11 917 0201

Country of Origin	Republic of South Africa
Year of Construction	2017
Manufacturer's No.	4944
Design Code	SANS 10131:2004
Design Pressure	ATMOSPHERIC kPa/g
Design Vacuum	kPa/g
Nominal Length	6600 mm
Nominal Diameter	2870 mm
Nominal Capacity	39
Leak Test Pressure	45 m3
Operating Pressure	ATMOSPHERIC kPa/g
Final Inspection Date	kPa/g
	16.10.2017
Manufacturer's Q.A. Stamp	[illegible]
Testing Institution Stamp	

Name Plate on the Tank

FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

OIL SKIMMER

- Oil Skimmer and underground Oil spillage drain was not found.

PUMPS

- Maintenance is required on the pumps.

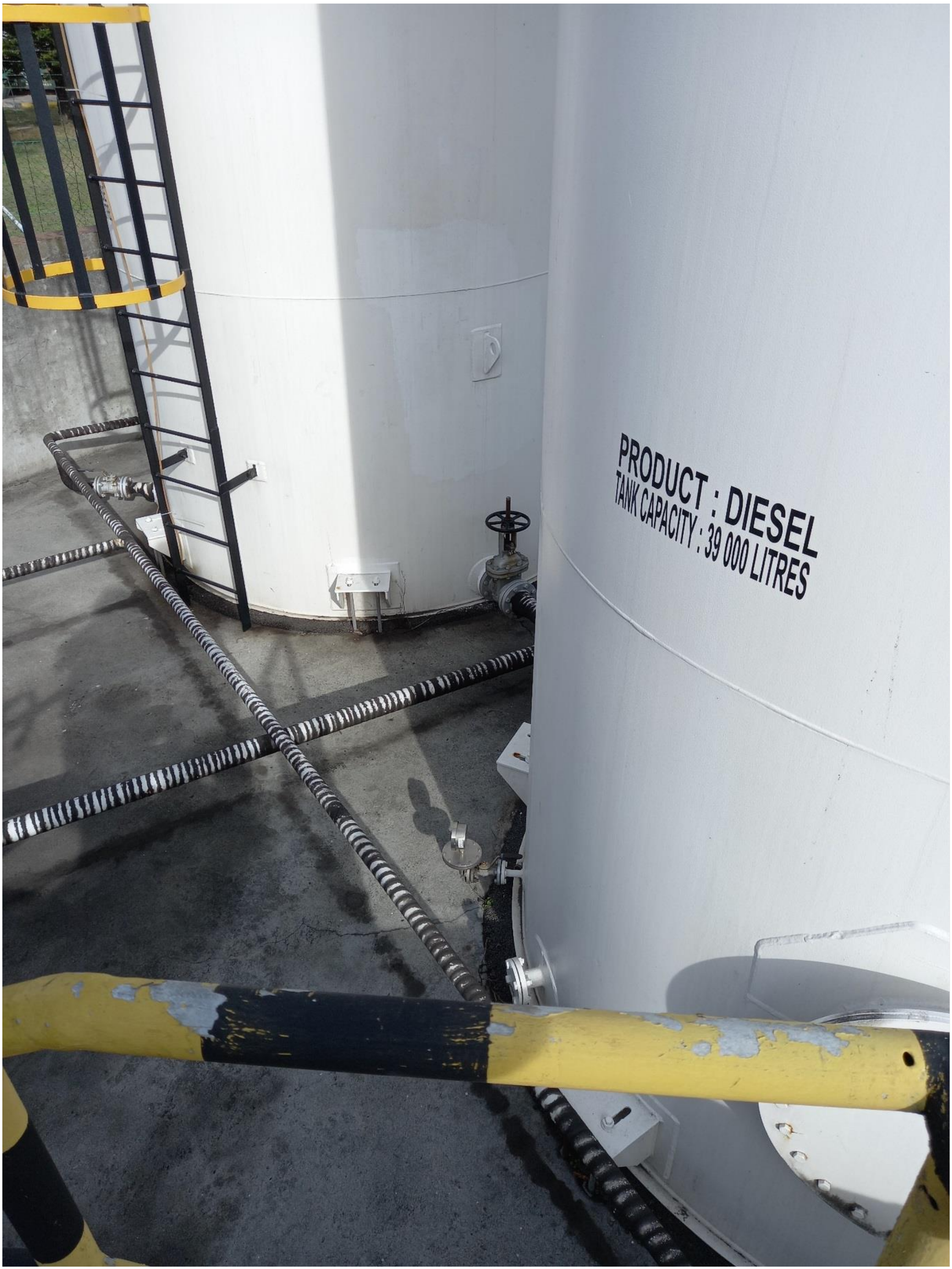
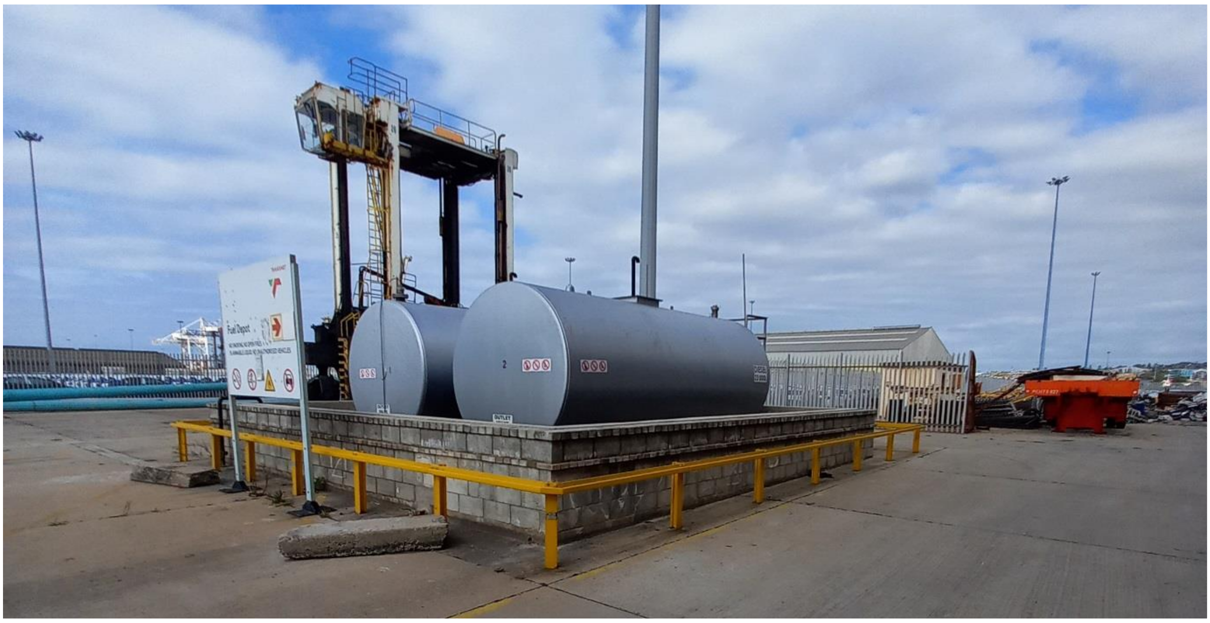


Photo of inside bunded area reflecting piping and hand railing

GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Tank needs to be washed /rinsed everyday due to excessive corroded condition.

6.7 PORT ELIZABETH



2 x 23 000 L horizontal Aboveground Tank: Diameter 2.3 m x 5.4 m Long

TANKS

- Two horizontal Aboveground Diesel Tanks were visually inspected on site including piping and other accessories.
- Tank is mounted on the support, which was not welded properly.
- Each tank has Diesel capacity 23 000 L with size 2.3 m diameter and 5.4 m long.
- Tank Manufacturer: unknown
- Paint/ coating was in a bad condition at multiple locations.
- Nozzles are in a good condition.
- Corrosion was spotted at various locations.
- MHI is required.

ELECTRICAL

- Wiring and DP was below the dispenser and needs urgent attention to rectify.
- Earthing cables needs to be organized.

INSTRUMENTATION

- All Instruments needs to be tested, calibrated, and certified.

- Level indicator/ gauge needs to install.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder needs complete coating.
- No top landing platform was identified.
- Steps sizes are incorrect and too small to climb the platform.
- Steps to enter the bund are also small and don't have handrails.

CIVIL WORKS

- Bund walls are in a good condition.
- Bund size: 7.6 m wide x 8 m long x 1 m height
- Bund area was clean.
- No vegetation was found around the bunded area.
- Drain from storm water was identified as a small hole to the bund are.

FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.
- Firefighting system was blocked by the huge vehicles (photo attached).

OIL SKIMMER

- No Oil/fuel spillage drain was found in the bunded area.
- Oil spillage tank area was in a mess (scrap was found around it).

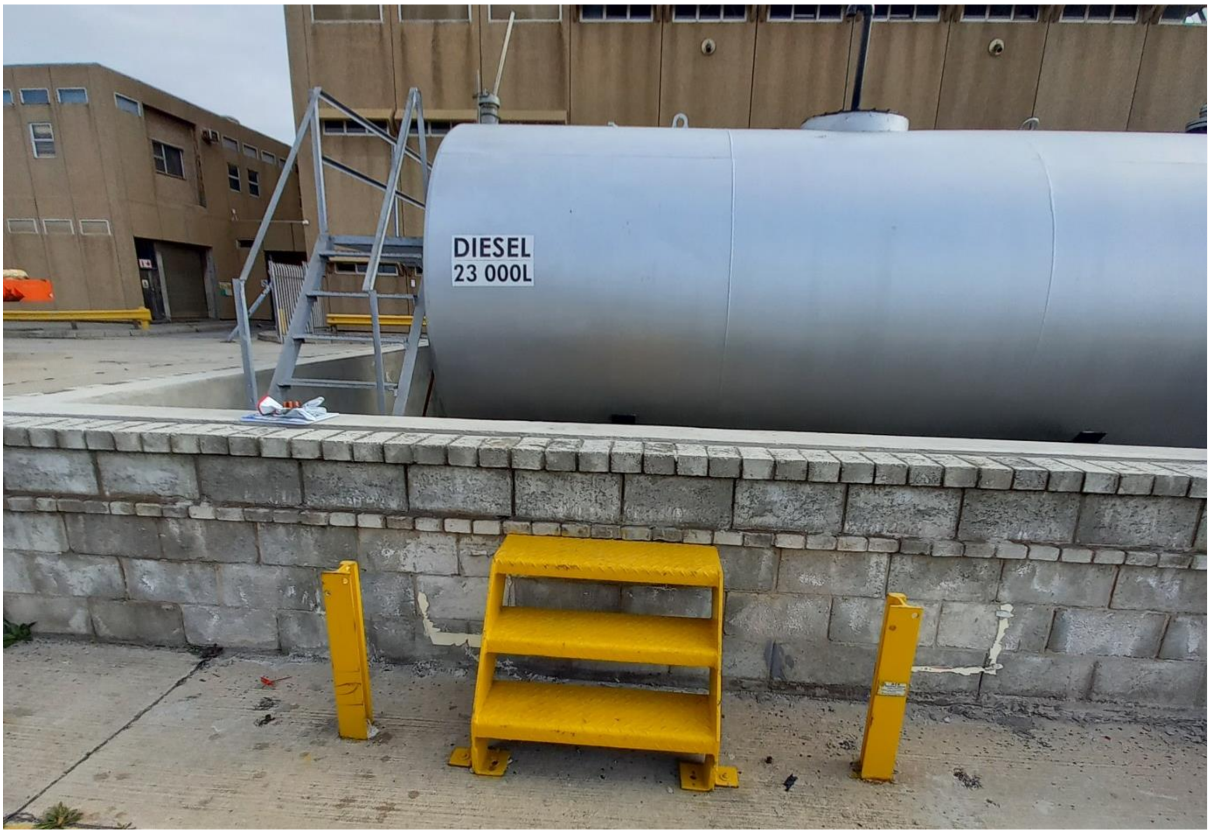
PUMPS

- Maintenance is required on the pumps.

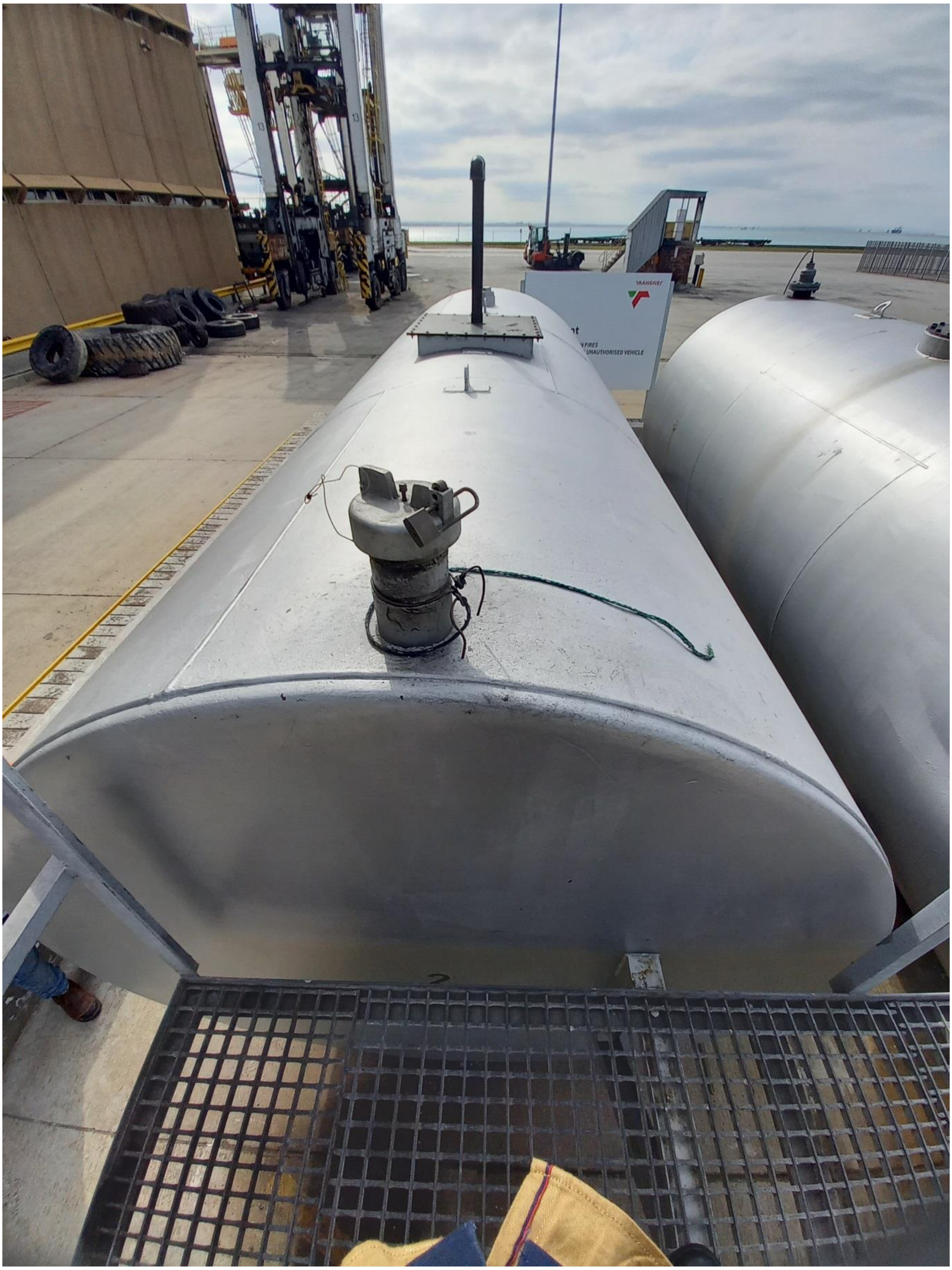
GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.

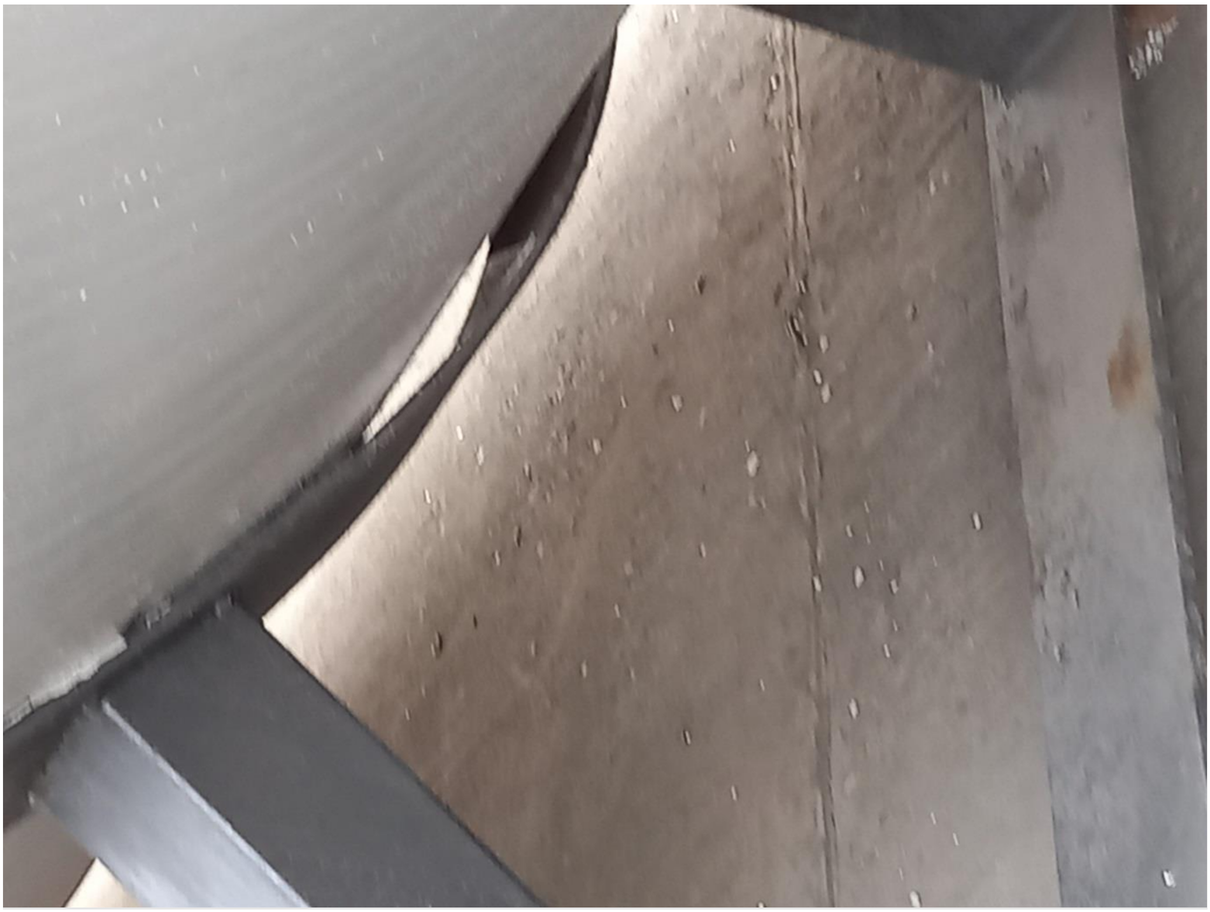
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Tank needs to be washed/ rinsed everyday due to excessive corroded condition.



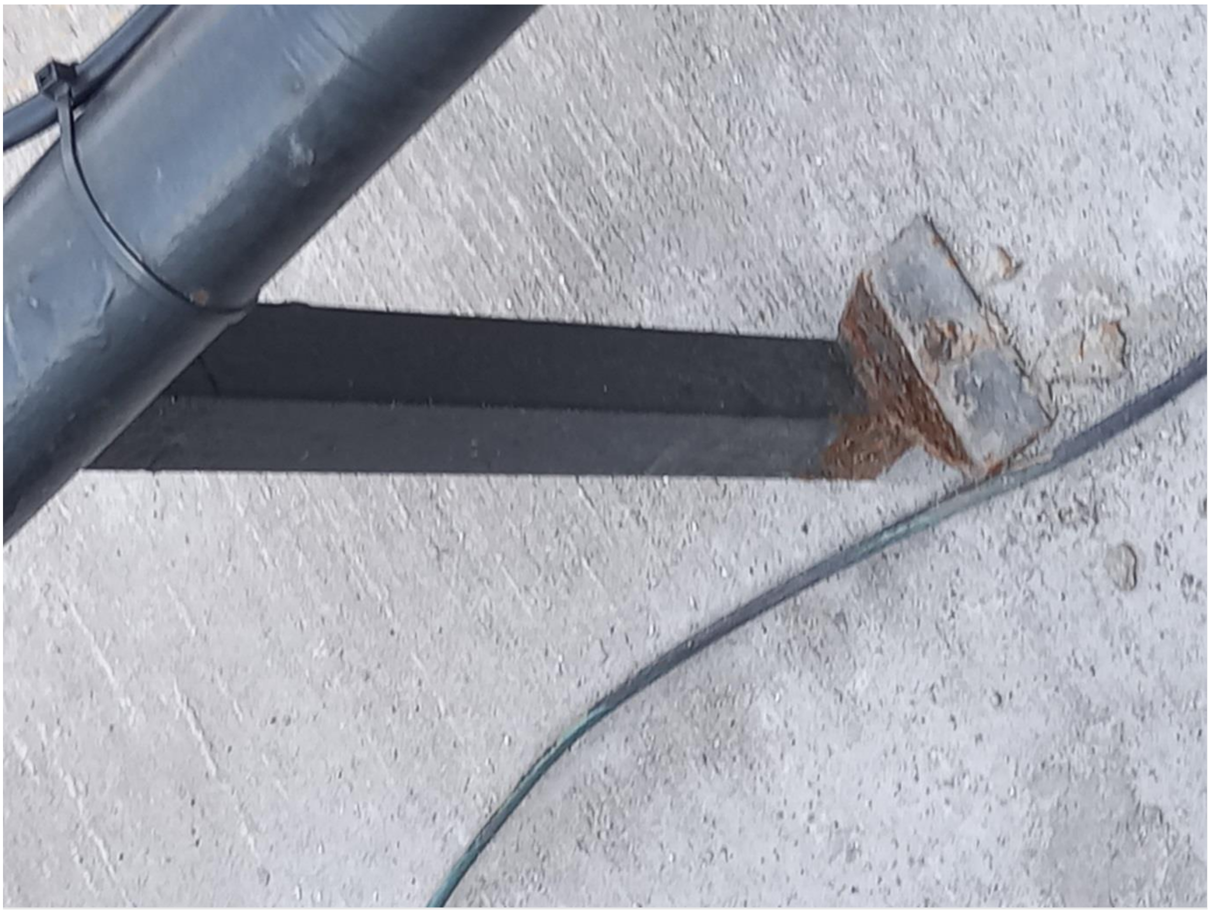
Small size and short steps with no handrails



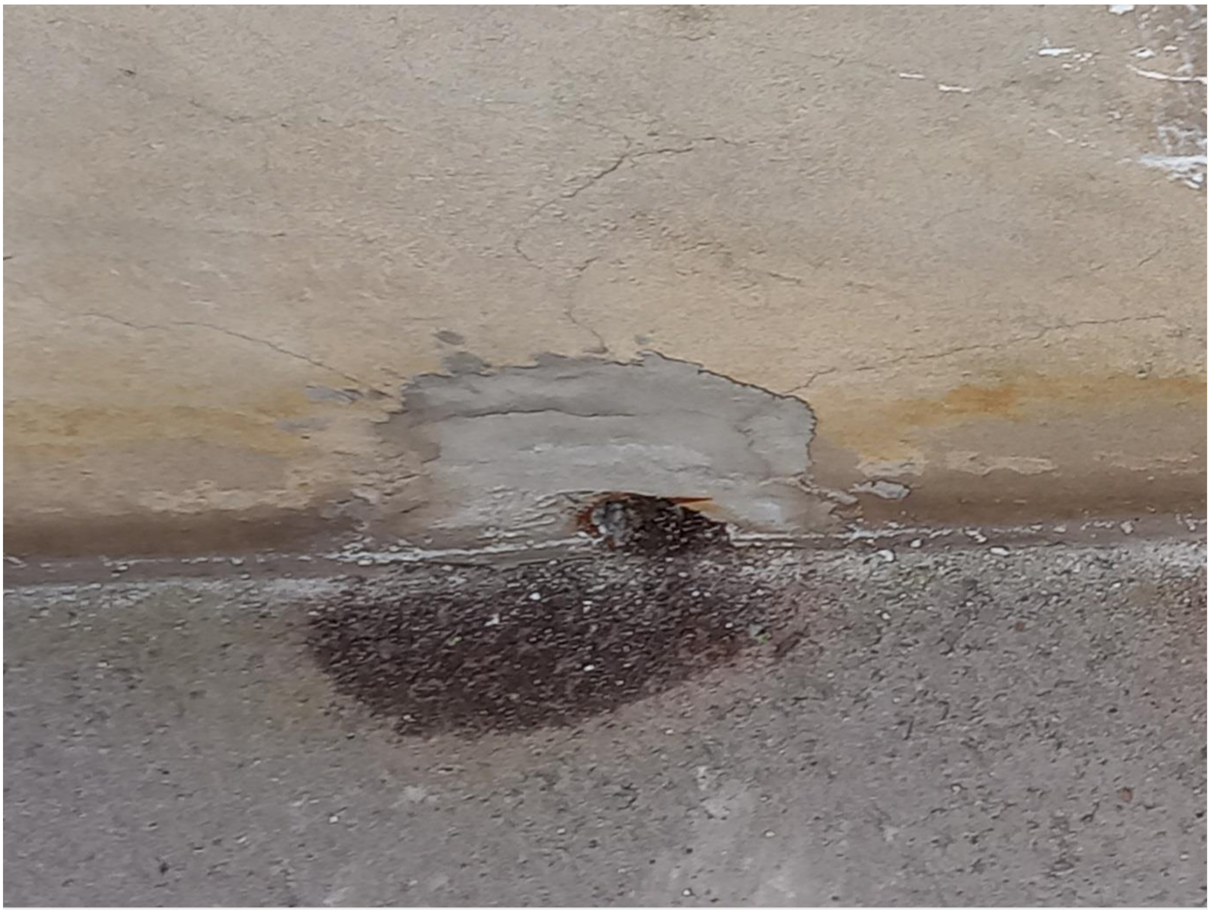
No extended platform to operate/repair/ maintain the nozzles on the top



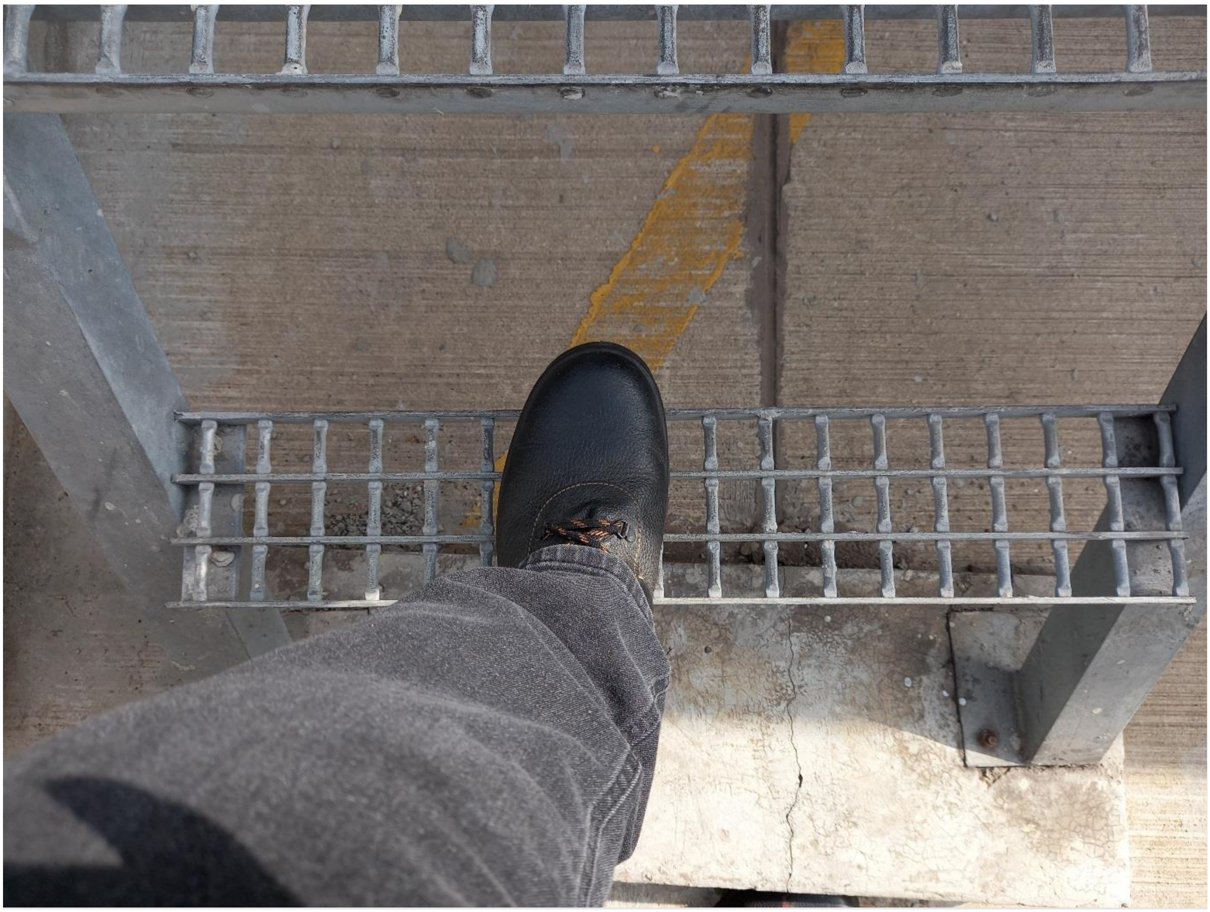
Vessel is not welded to the support



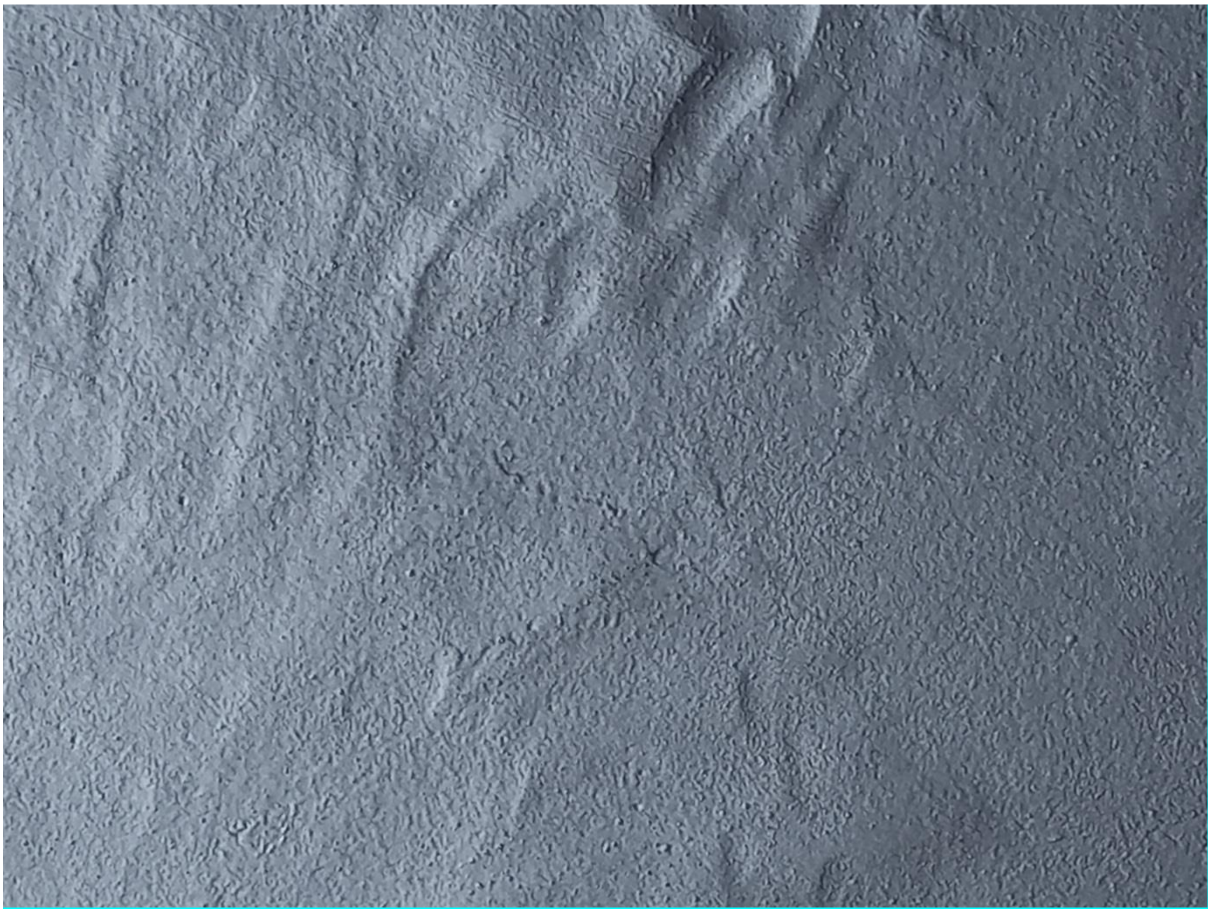
Piping supports needs to be replaced



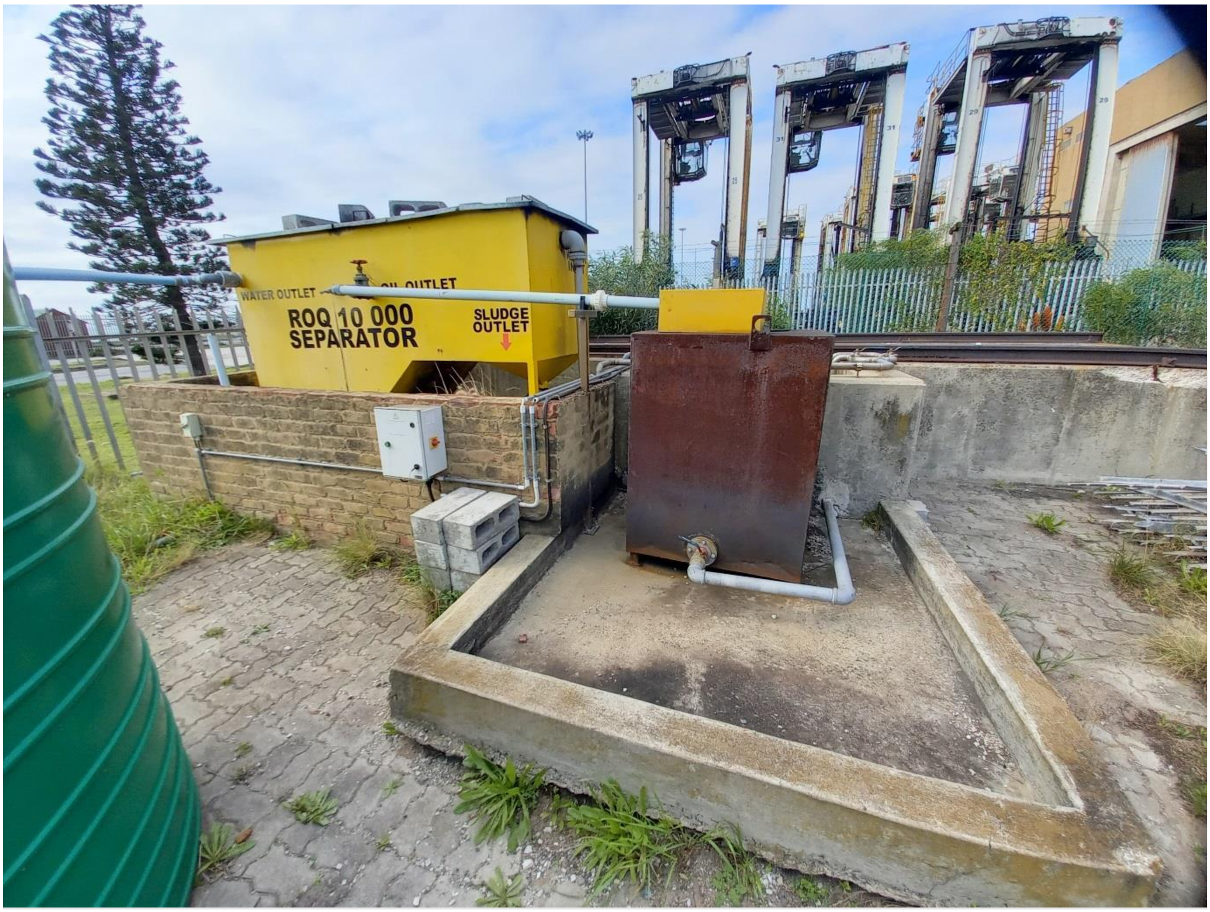
Storm water drain hole



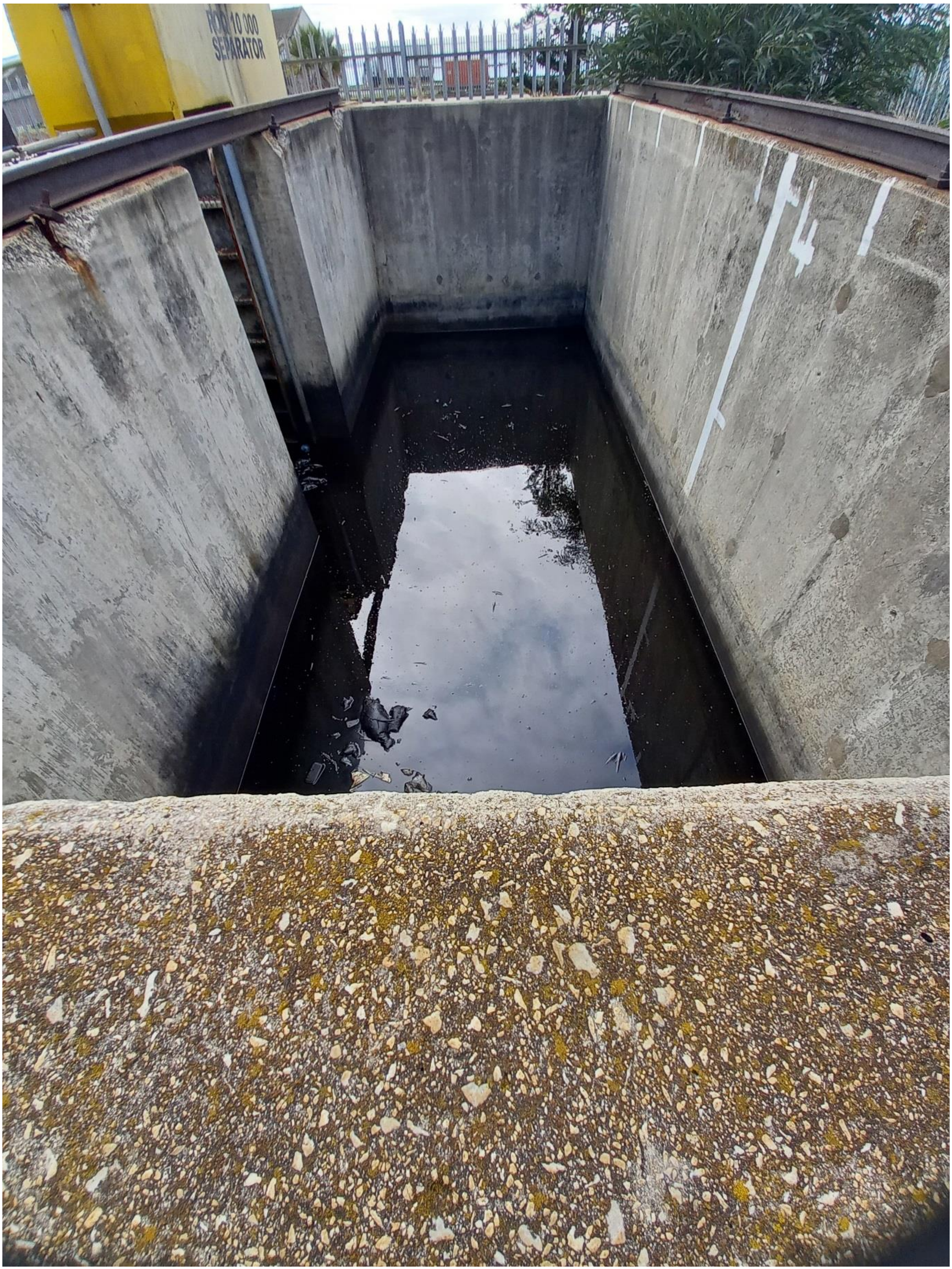
Shot and small step



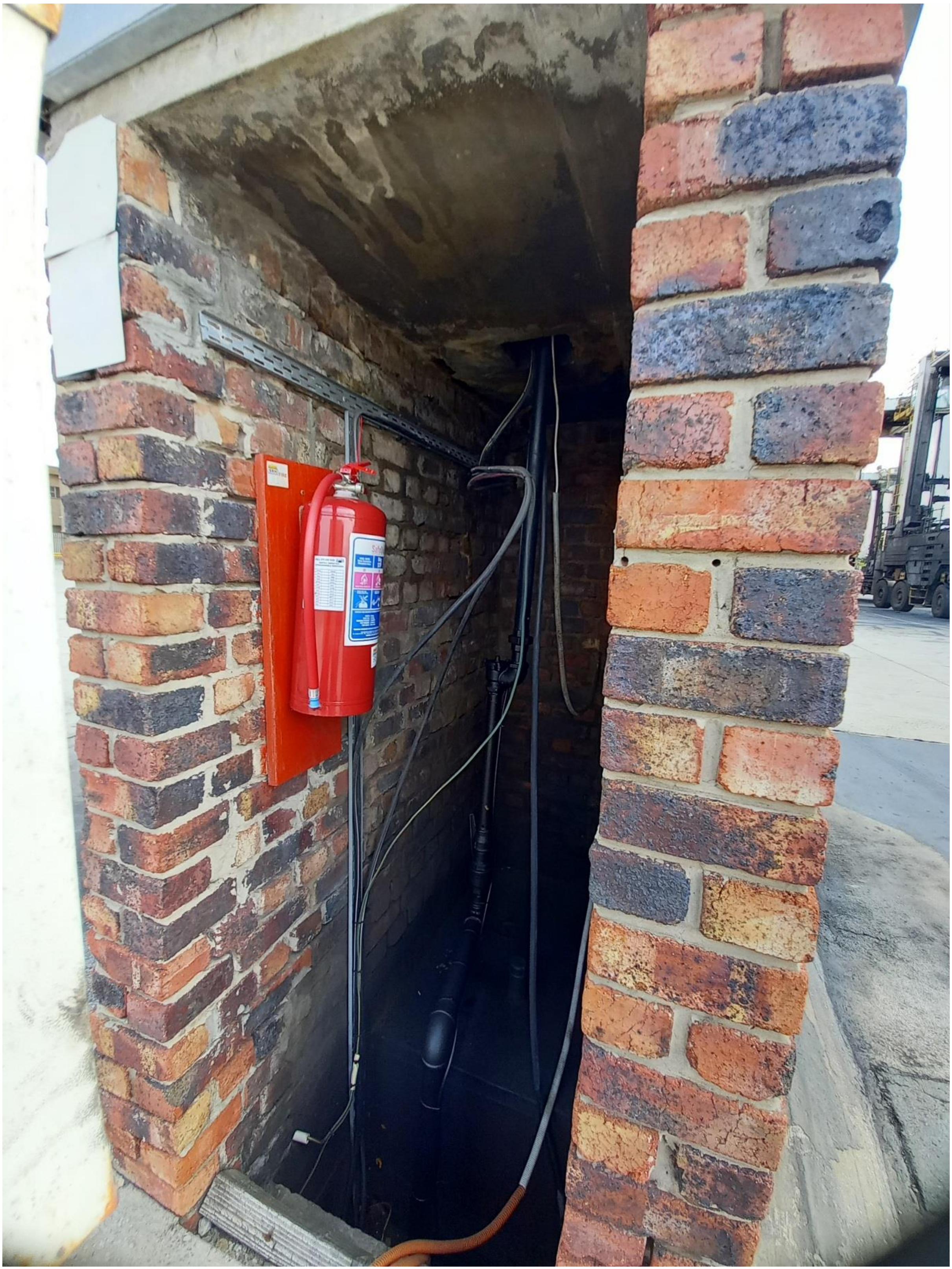
Painting in a bad condition: photo of dished end Surface



Oil spillage collection and filter area

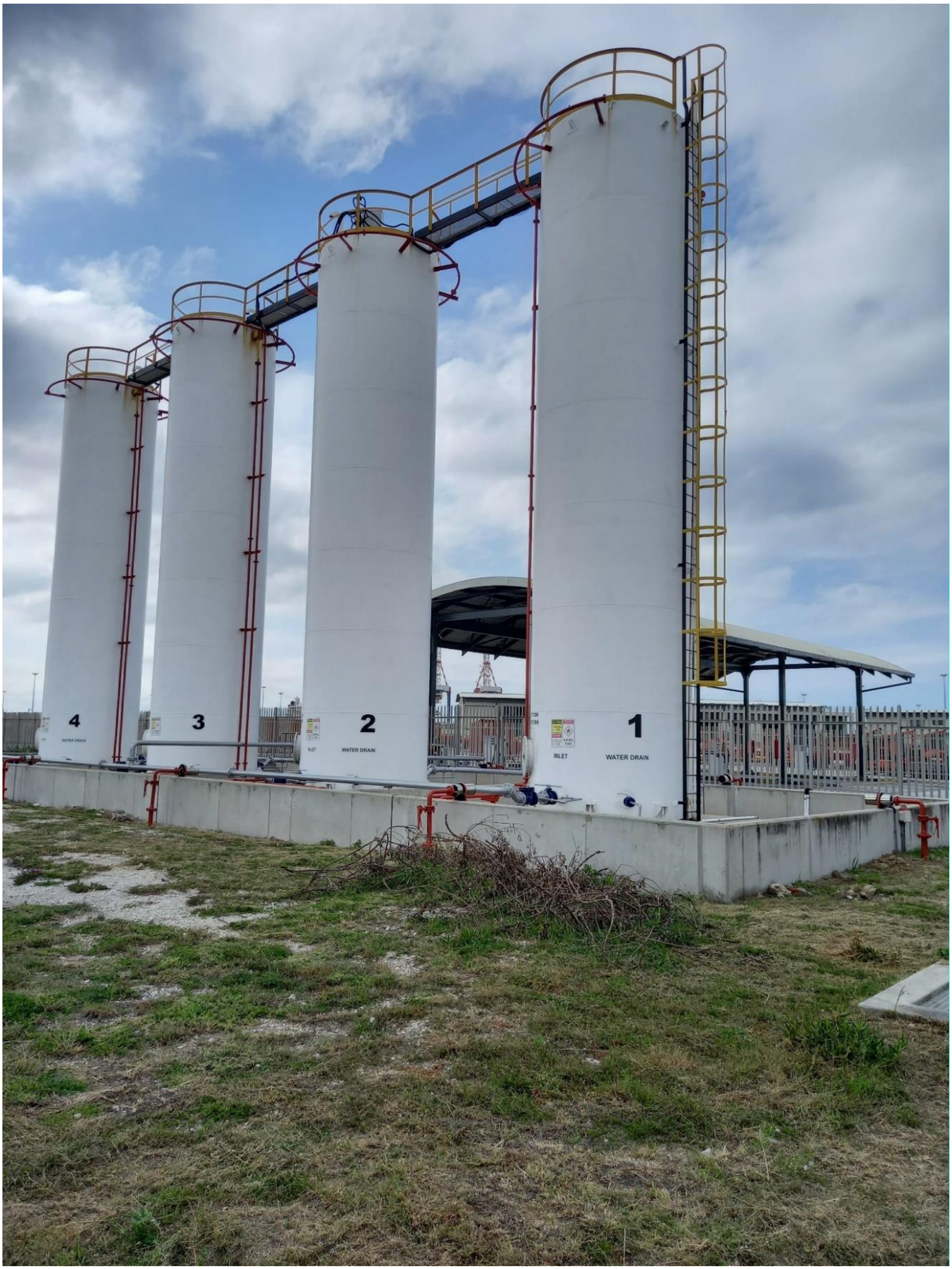


Oil spillage collection



Electrical cables: urgent attention is required

6.8 NGQURA CONTAINER TERMINAL (NCT)



63 000 L – 4 x Diesel Tanks

TANKS

- Four Vertical Aboveground Diesel Tanks were visually inspected on site including piping and other accessories.
- Tank is mounted on the annular ring which had a Denso wrapping.
- Each tank has Diesel capacity 63 000 L with unknown size. The capacity written on the Tank and name plate doesn't match with each other.
- Tank Manufacturer: Forgeweld Engineering
- Paint/ coating was in a bad condition at multiple locations.
- Nozzles are corroded.
- Corrosion was spotted at various locations.
- MHI is required.

ELECTRICAL

- Wiring and DP was in a good condition.
- Earthing cables needs to be organized.

INSTRUMENTATION

- All Instruments needs to be tested, calibrated, and certified.
- Level indicator/ gauge needs to install.
- Tanks are getting overfilled.

PLATFORMS, LADDERS AND STRUCTURAL

- Ladder needs complete coating.
- Landing platform was missing.

CIVIL WORKS

- Bund walls are in a good condition.
- Bund area was clean.
- Vegetation was found around the bunded area.
- Storm water drain was full of water.

FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

- Foam Water Tank Pumps DP is locked by TNPA; hence we were unable to check the condition.
- Foam water system is getting heavily rusted and urgent attention is required.

OIL SKIMMER/ FILTRATION

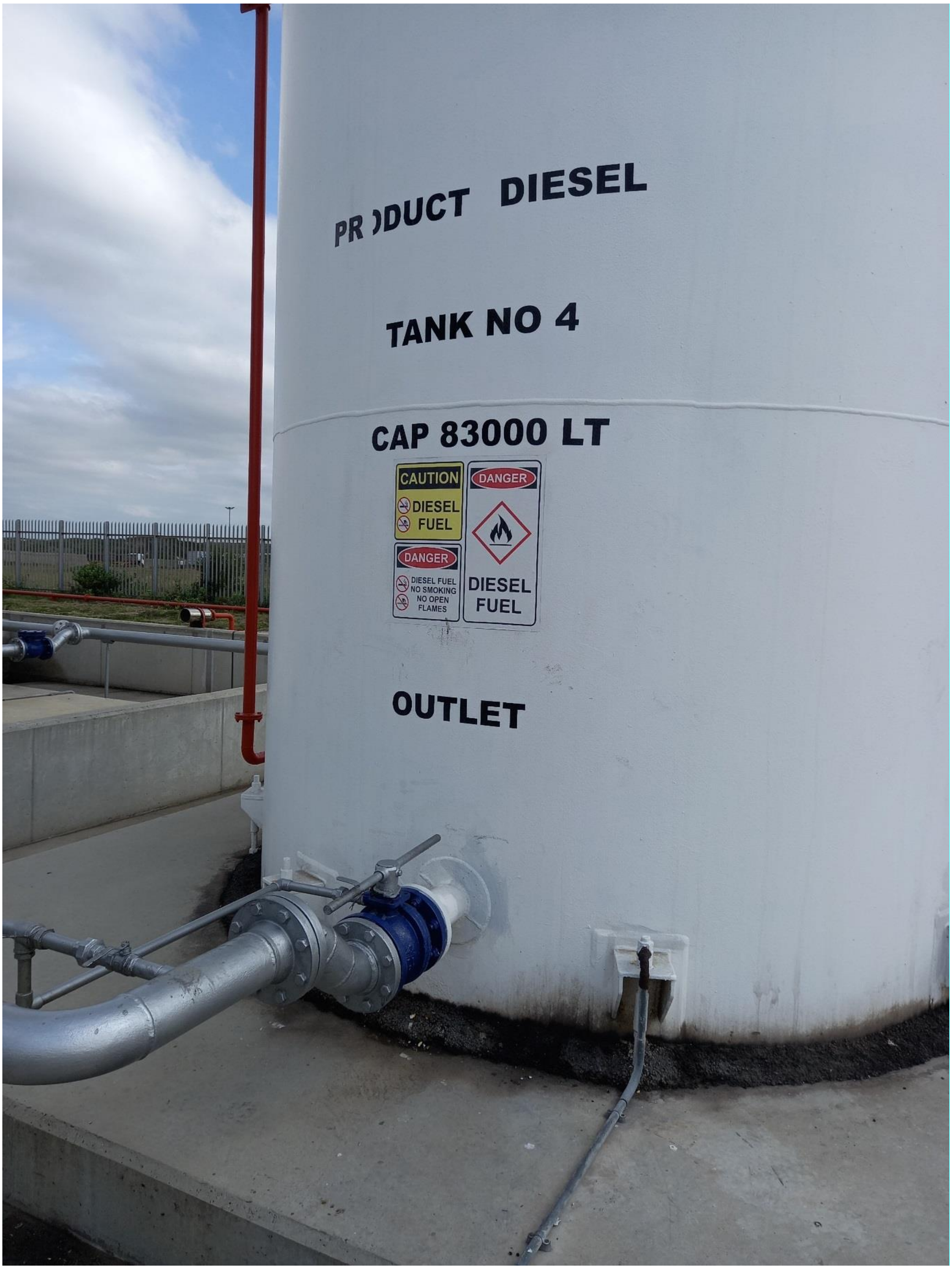
- No oil skimmer or oil filtration plant was identified.
- Oil spillage Tank was in a good condition.

PUMPS

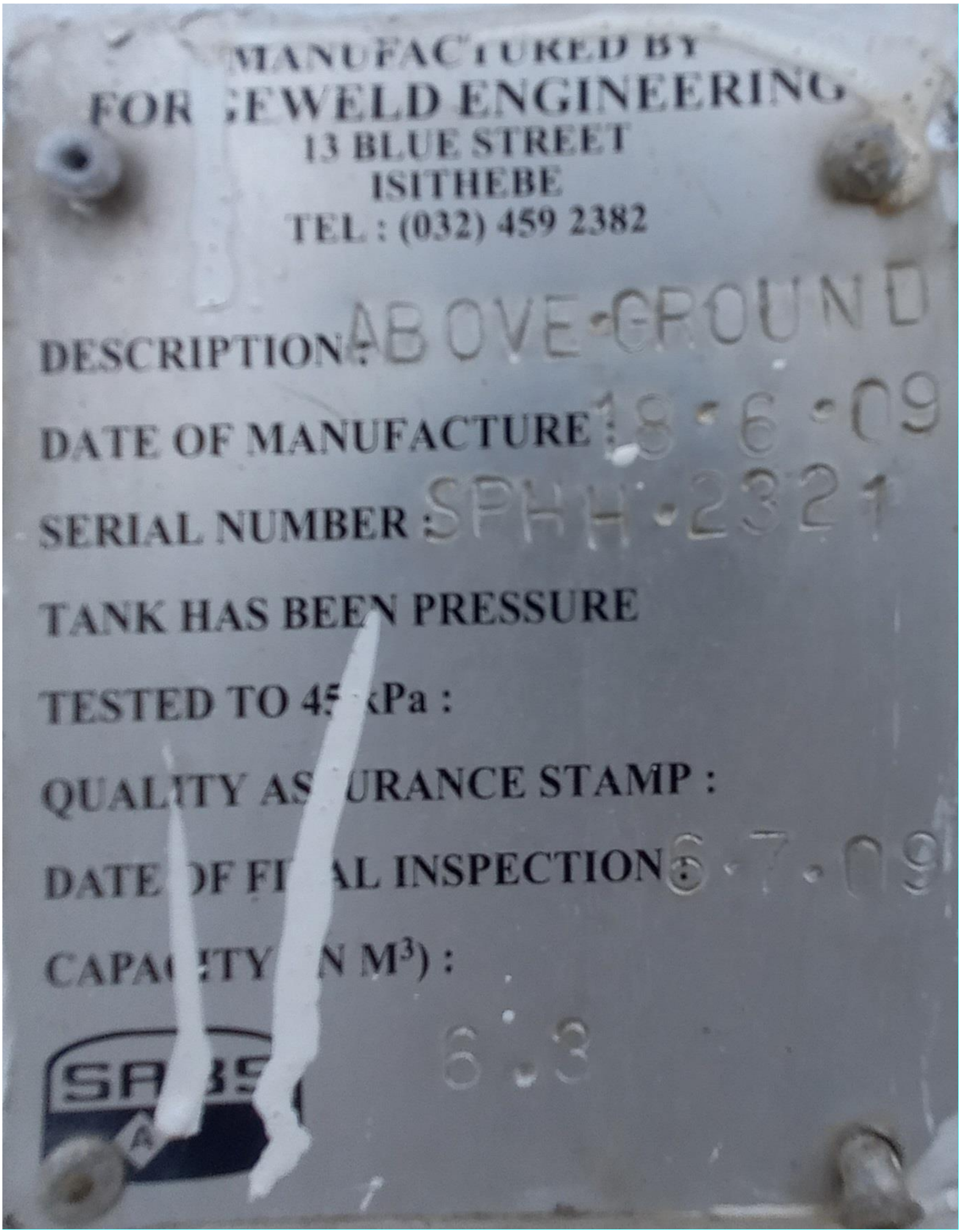
- Maintenance is required on the pumps.

GENERAL OBSERVATION

- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Tank needs to be washed/ rinsed everyday due to excessive corroded condition.



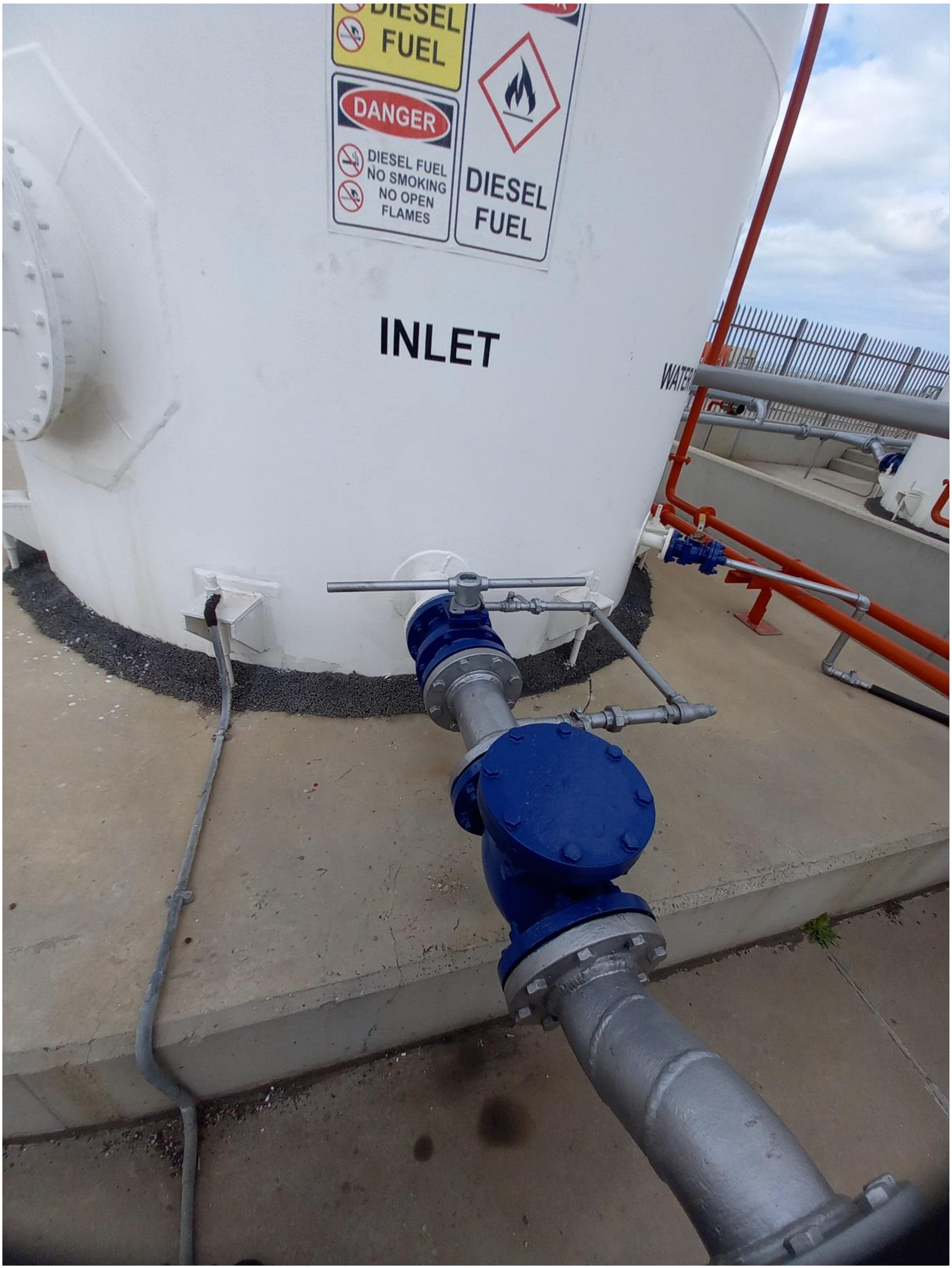
Close up photo of tanks with annular ring, earthing cables and outlet nozzle



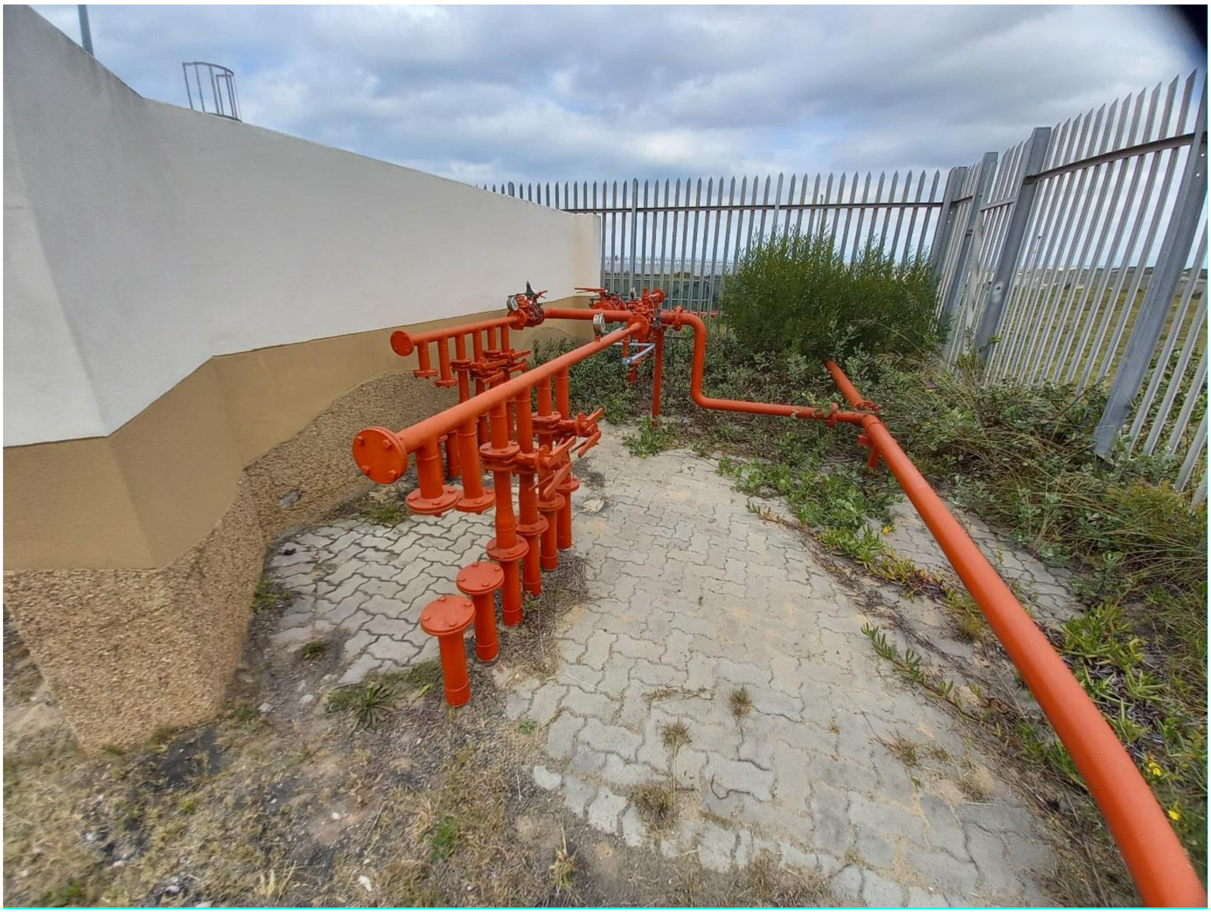
MANUFACTURED BY
FORGEWELD ENGINEERING
13 BLUE STREET
ISITHEBE
TEL : (032) 459 2382

DESCRIPTION : ABOVE-GROUND
DATE OF MANUFACTURE : 18-6-09
SERIAL NUMBER : SPHH-2321
TANK HAS BEEN PRESSURE
TESTED TO 45 kPa :
QUALITY ASSURANCE STAMP :
DATE OF FINAL INSPECTION : 6-7-09
CAPACITY (IN M^3) :
6.3

Name Plate of the Tank with 6.3 000 L Capacity



Tank Inlet nozzle



Firefighting piping

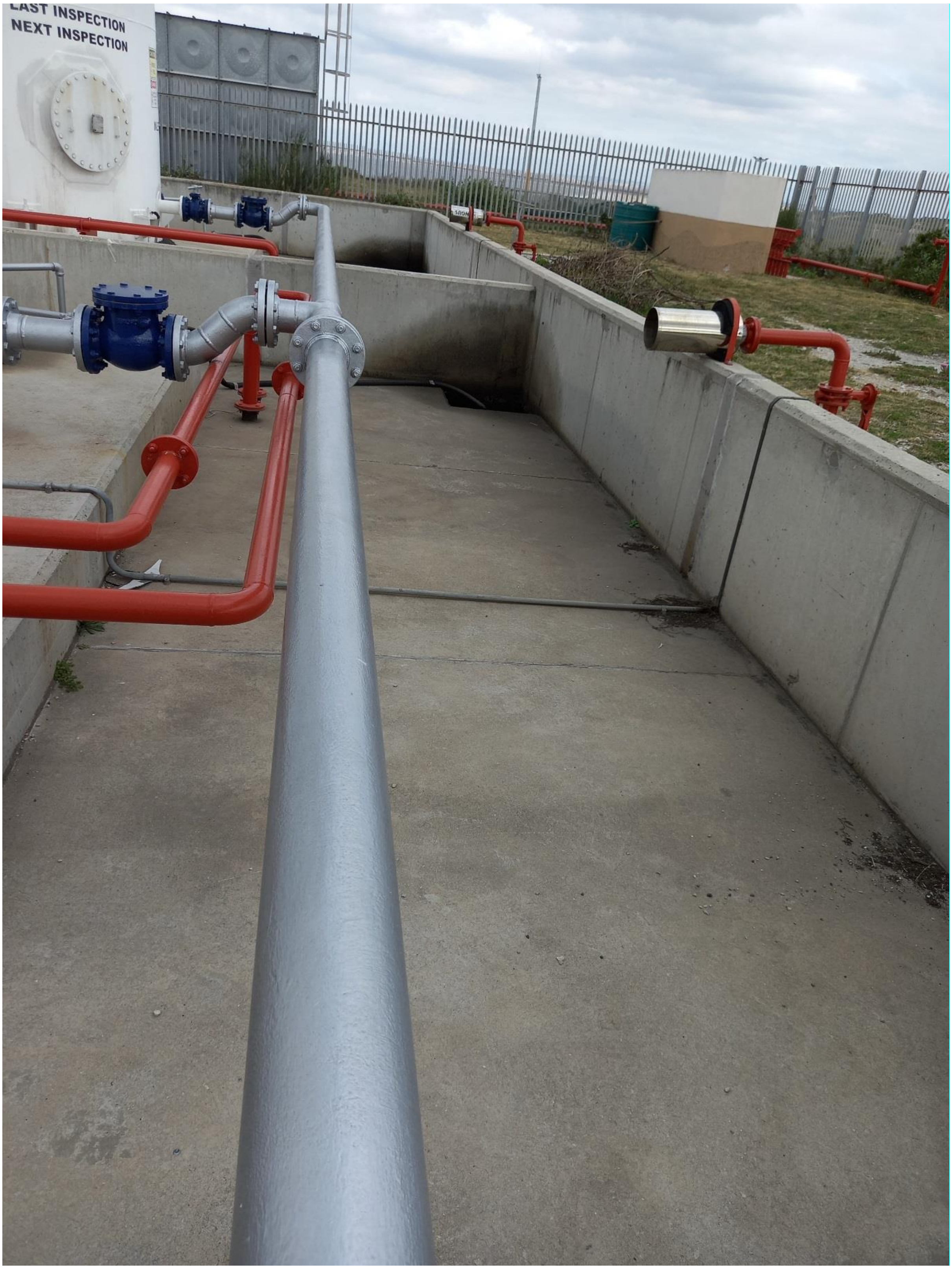
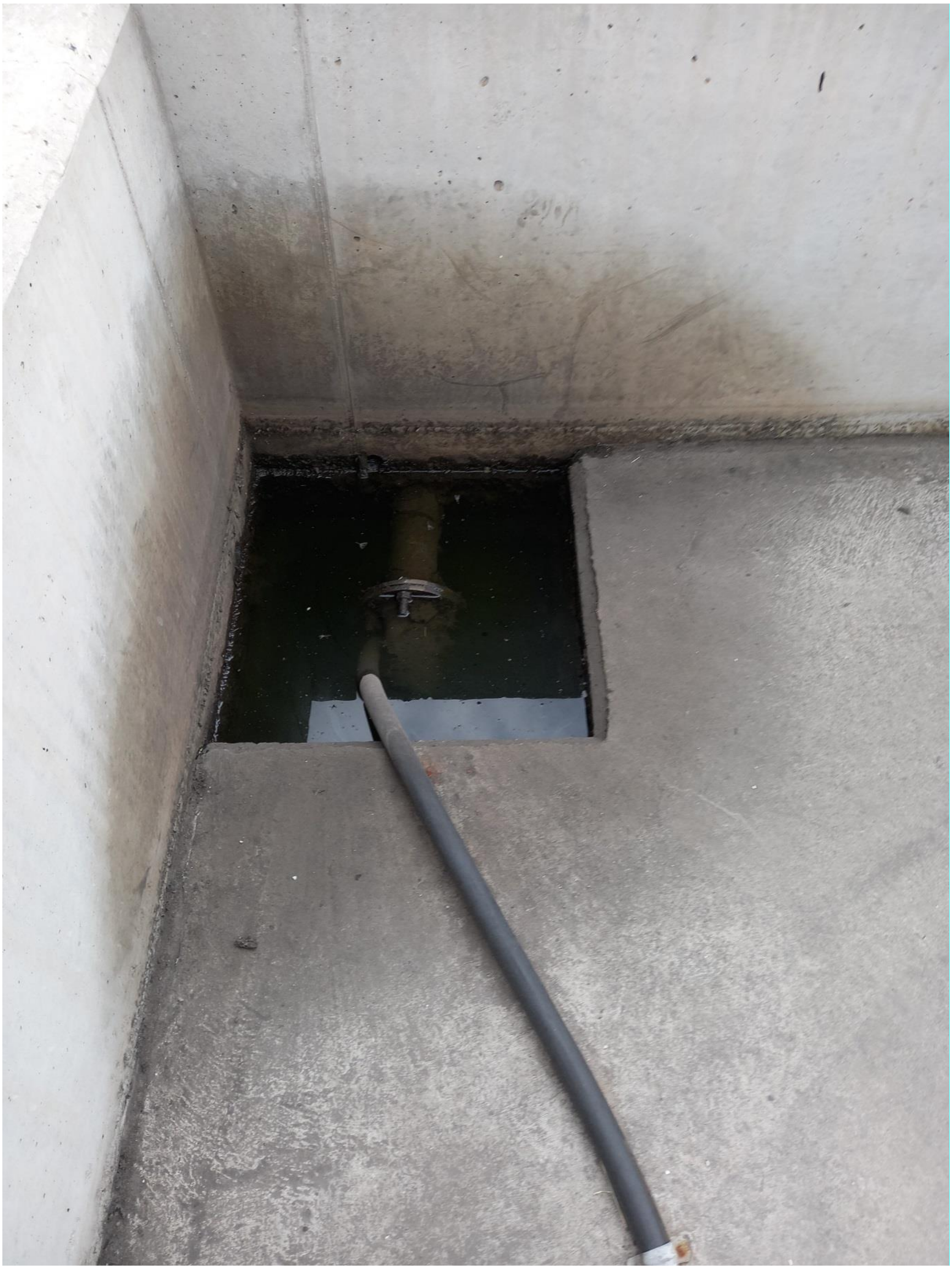
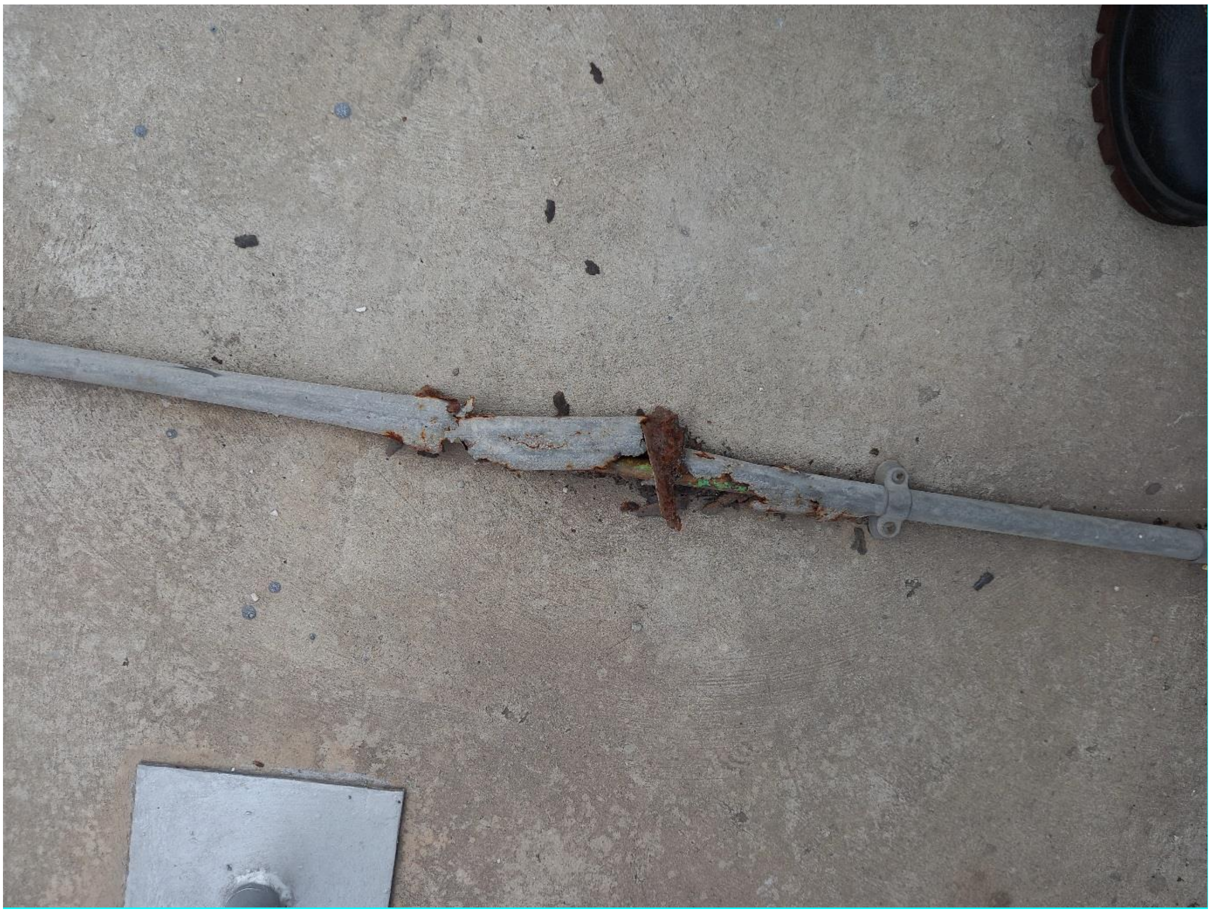


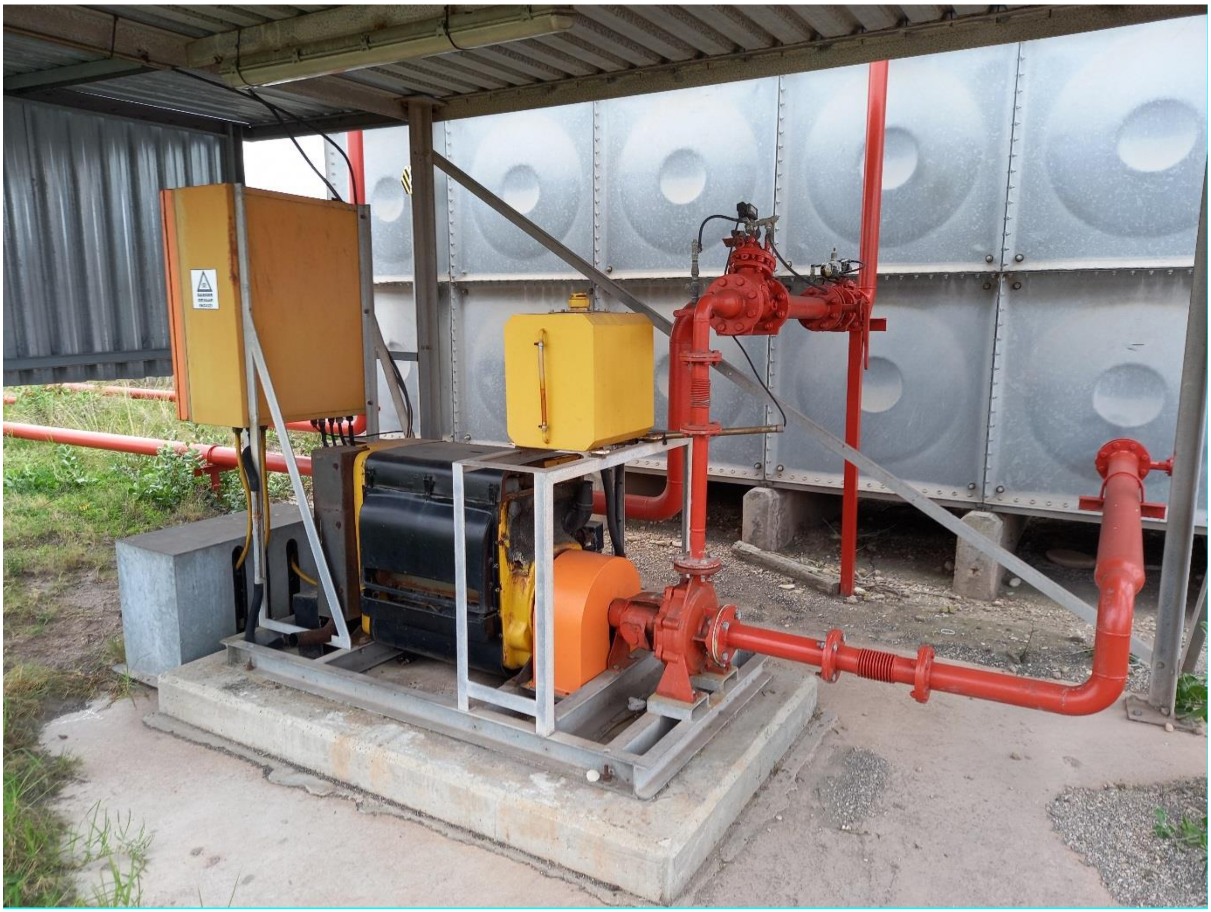
Photo of bund area



Strom water drain is chocked



Earthing cable cover is broken and in a poor condition



Foam Water supply system

6.9 EAST LONDON

Below ground 4 Tanks: 2 Diesel and 2 Petrol (14 000 L each)

TANKS

- Two horizontal below ground Tanks were identified on site including piping and other accessories.
- 2x Diesel Tanks capacity: 23 000 L each with sizes unknown.
- Both Petrol Tanks failed in the inspection and needs to be removed.
- Tank Manufacturer: unknown

ELECTRICAL

- Wiring and DP was in a good condition.

INSTRUMENTATION

- All Instruments needs to be tested, calibrated, and certified.

PLATFORMS, LADDERS AND STRUCTURAL

- N/A

CIVIL WORKS

- N/A

FIRE FIGHTING

- Firefighting system needs to be verified as per NFPA, SANS, API and OSH Act requirements.

OIL SKIMMER / FILTRATION

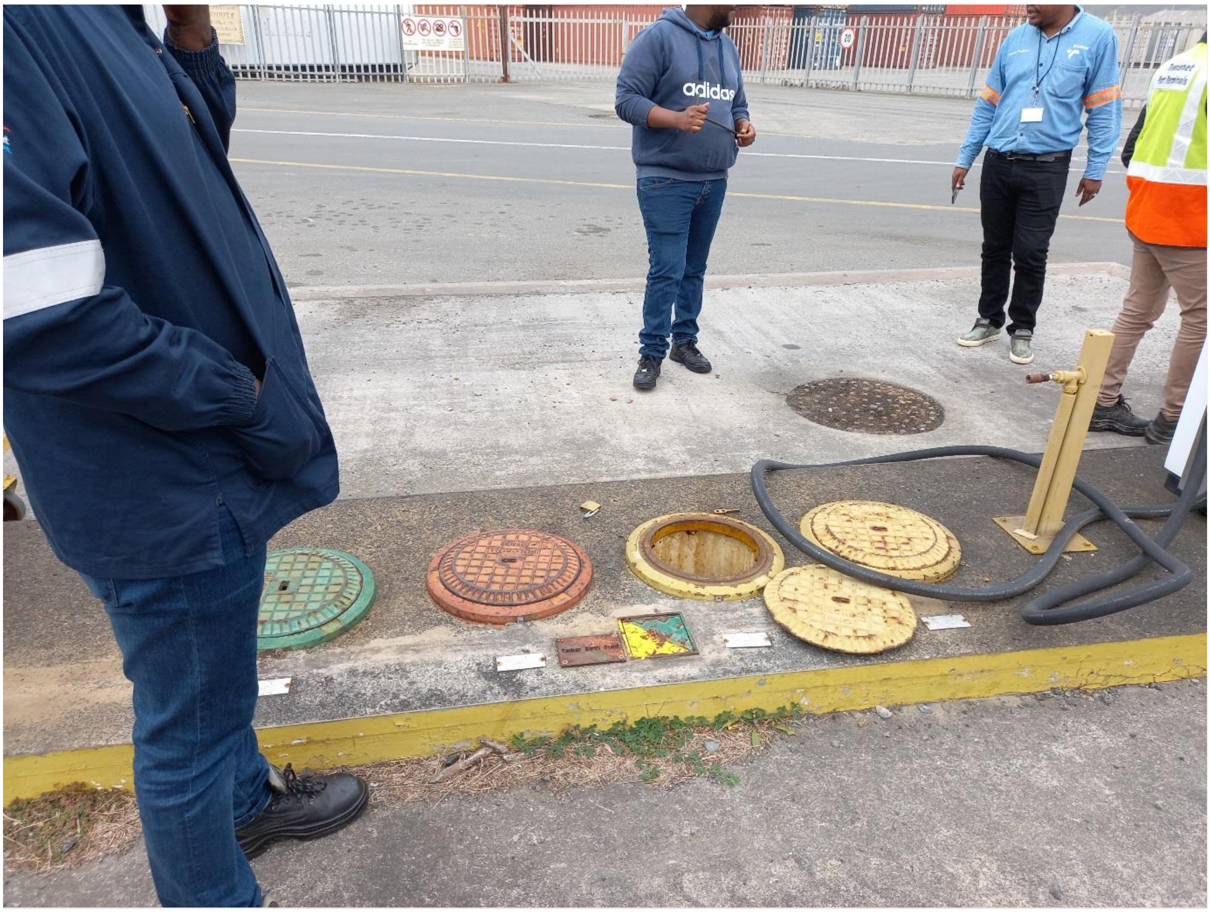
- Oil Skimmer and underground Oil spillage drain was not found.
- Strom Water Drain was blocked.

PUMPS

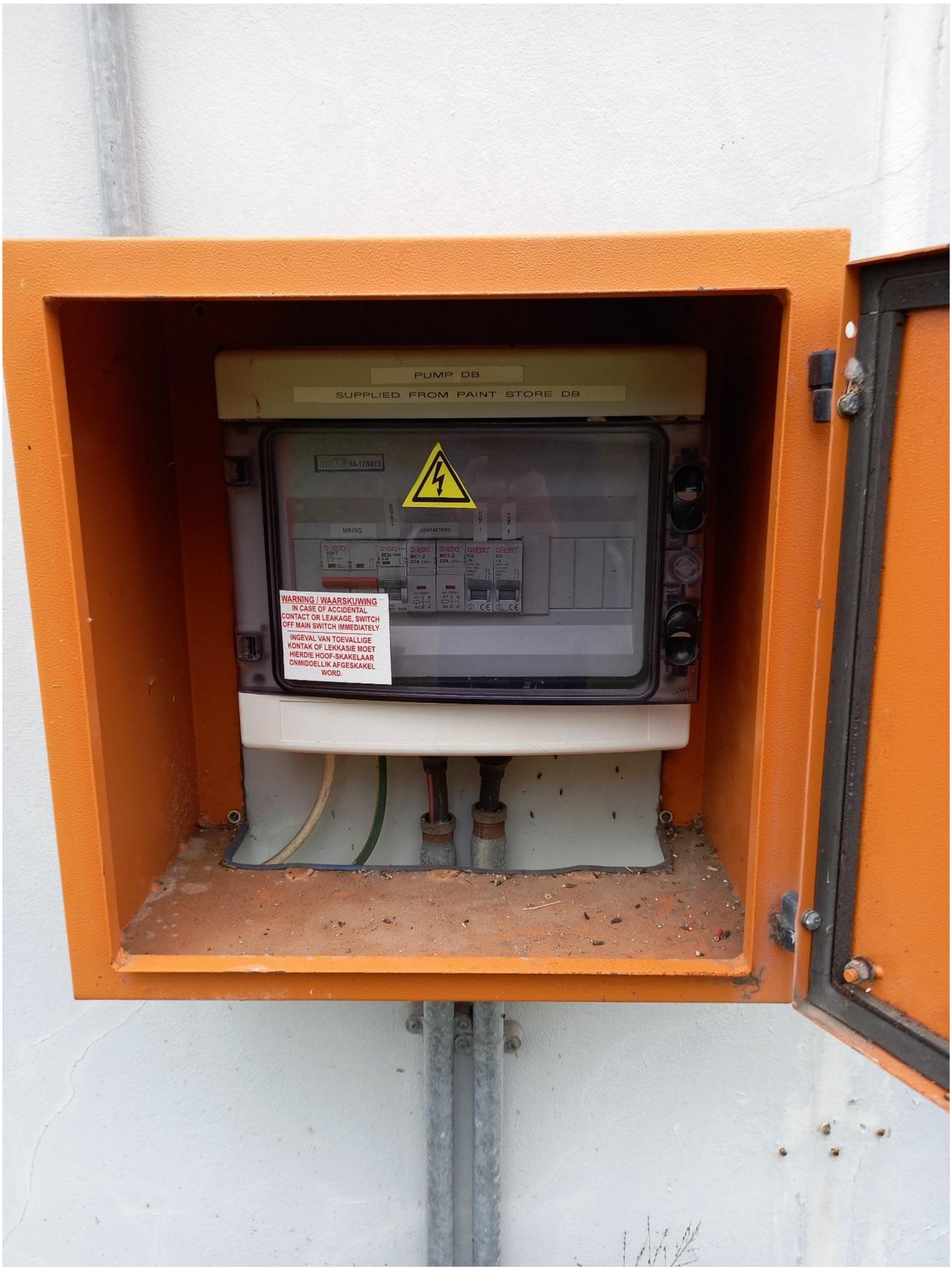
- N/A

GENERAL OBSERVATION

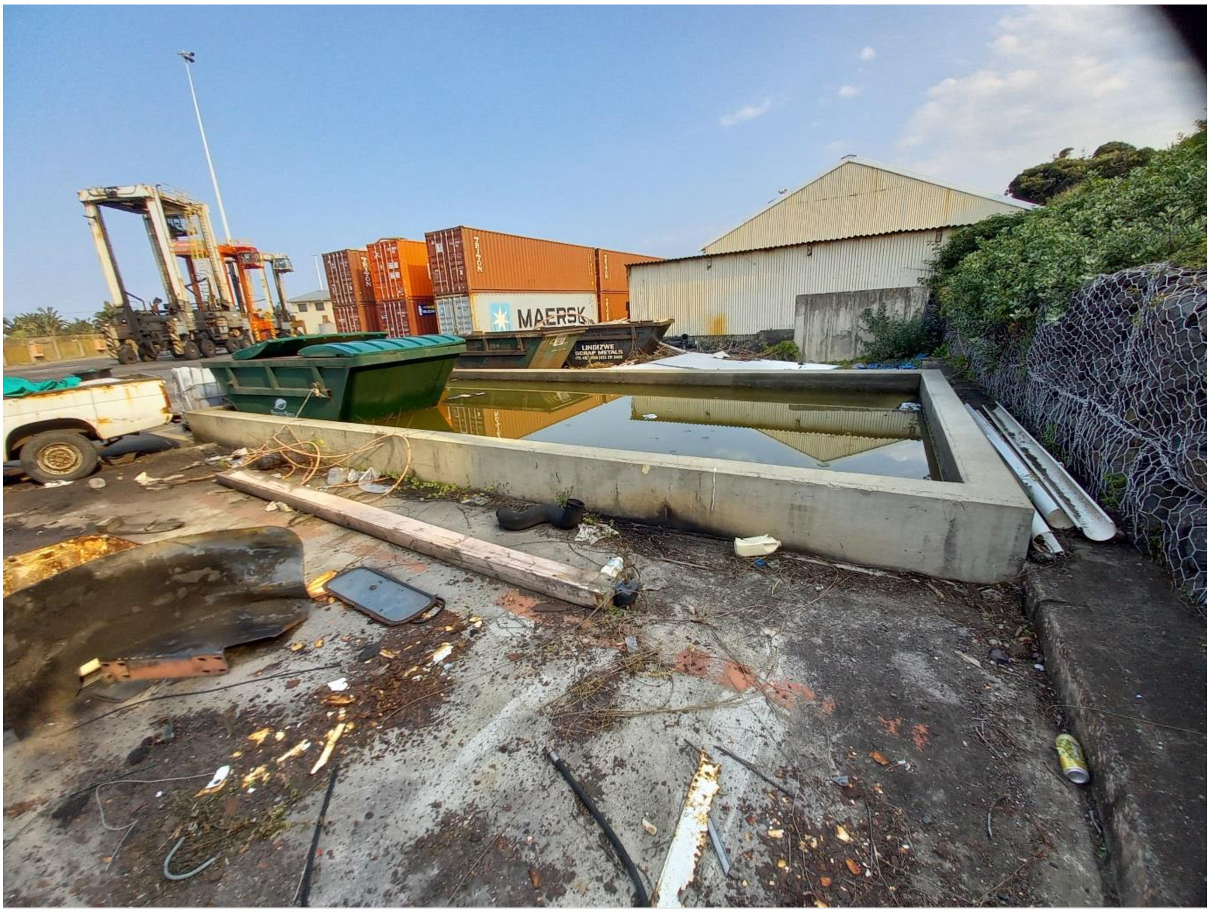
- Alternative area in the same premises was proposed to build the two new Diesel Tanks.
- Need proper colour coding for Tanks, Pipping, Structural and other accessories.
- Vegetation and untidiness around the Tank and Bund Area.
- Identification, Signage and Marking is required.
- No Layout drawing found.
- No record for testing of the Tanks as per regulation was found.
- No record for calibration of instruments was found.
- No record of operation or maintenance for the Tanks & the facility was found.
- No Drawings, Data books or certificates were found.
- No repair and alteration record found.
- No maintenance plan found.
- No Risk Assessment Report found.
- No Environmental compliance report found.
- Fuel Pump calibration certificates not available.
- Tank needs to be washed/ rinsed everyday due to excessive corroded condition.



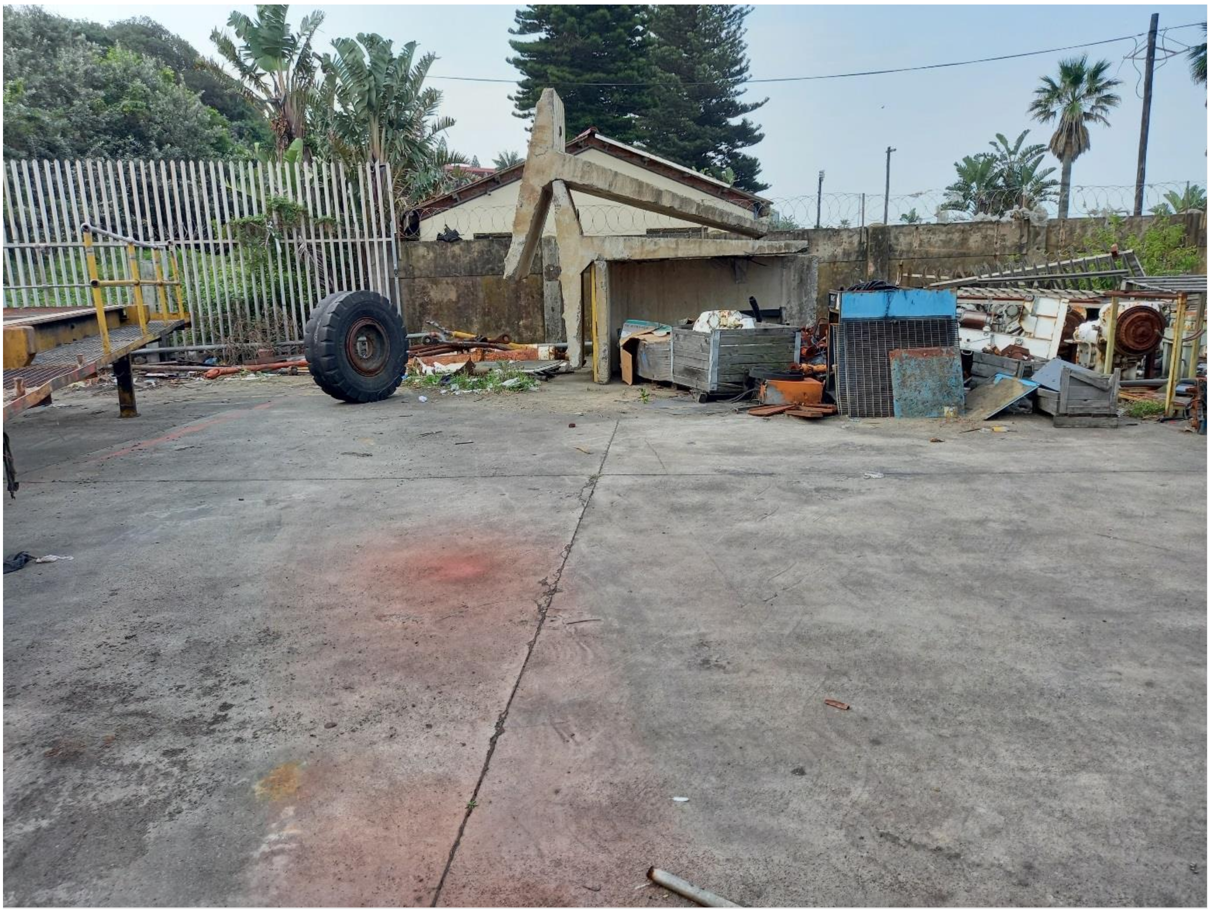
Four underground Tanks


PUMP DB
SUPPLIED FROM PAINT STORE DB
MAINS
CONTACTORS
WARNING / WAARSKUWING
IN CASE OF ACCIDENTAL CONTACT OR LEAKAGE, SWITCH OFF MAIN SWITCH IMMEDIATELY
INGEVAL VAN TOEVALLIGE KONTAK OF LEKKASIE MOET HIERDIE HOOF-SKAKELAAR ONMIDDELLIK AFGESKAKEL WORD.

Distribution Board in an excellent condition was found



New area proposed to build the Tanks: severe cleaning is required.



Alternative area for constructing New Diesel Tanks

7. COST AND SCHEDULE

7.1 COST TABLE

The cost includes repairs to Fuel Tank, Tank Access Platform, Electrical, Instrumentation, Civil Works, Fire Fighting System, Pumps, and hired fuel tank.

#	Item	Total cost
1.	**New Installations at Pier 1, East London & Saldanha**	
1.1	Supply and install Fuel Tanks • Pier 1: 50 000L x 2 • East London: 35 000L x 1 • Saldanha: 35 000L x 1	R7 500 000
1.2	Remove the existing Tank	R1 250 000
1.3	Civil Work	R3 600 000
1.4	Electrical Work	R1 500 000
1.5	Mechanical Work & Fire System	R2 400 000
2.	**Sub Total**	**R16 250 000**
3.	**Repairs**	
3.1	Repairs to the tank	R8 000 000
3.2	Civil Work	R2 100 000
3.3	Electrical Work	R2 100 000
3.4	Mechanical Work & Fire System	R2 100 000
3.5	Hire Fuel Tank	R890 000
4.	**Sub Total**	**R14 300 000**
5.	Preliminaries and General (20%)	R6 110 000
6.	Disbursement (5%)	R1 527 500
7.	Tank Hire	R890 000
8.	**Total Direct costs**	**R39 108 050**
9.	**Indirect costs**	
10.	TPT Project Management Fee (as per Man-plan)	R4 001 893
11.	TPT Contingency (10%)	R3 910 805
12.	**Total Indirect costs**	**R7 912 698**
13.	**Total cost**	**R47 020 748**

7.2 CASH FLOW

FY	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	TOTAL (Rm)
23/24					3,284	2,585	6,278	3,284	1,5	1,5	3,284	3,154	**23,869**
24/25	4,528	3,187	4,624	4,273	3,652	1,387	0.5						**23,151**
Total	**4,528**	**3,187**	**4,624**	**4,273**	**6,936**	**3,972**	**6,778**	**3,284**	**1,5**	**1,5**	**3,284**	**3,154**	**47,021**

7.3 SCHEDULE

Project Deliverables	Completion Date
ORS Classification	October 2022
Investment Forum	Nov 2022
CAPIC	Jan 2023
LOA	June 2023
Execution	Sept 2024
Project close-out	Nov 2024
CAN Expiry	Oct 2025

8. RECOMMENDATIONS

- Scope of Work to established by the entire team
- Commence with Phase 1 of the project to ensure regulatory compliance
- Award the Project as one contract to ensure uniformity across Terminals
- Finalize Fuel Capacity Strategy to ensure correct Tanks are manufactured if necessary
- Compile Project Execution Plan and share with the Terminals
- Operation and maintenance manuals to be written for each Port separately
- Provide operation and maintenance training after completing each Terminal
- Water and Oil spillage drains, collection Tank, Canopy/ Shade and filtration systems to be handled separately.

TRANSNET

Transnet Group

INFORMATION SECURITY POLICY

Policy Reference Number	*TG/EISM 8/4/3P*
Version Number	*3.0*
Effective Date	*March 2022*
Review Date	*March 2027*
Policy Owner	*GM: Cyber Security, Governance, Risk and Compliance*
Signature	Stephen Mark
Policy Sponsor	*Group Chief Information Officer*
Signature	
Date Approved	10/5/2022

Stakeholders

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Compulsory Stakeholder Involvement						
Subject Matter Experts	Daniel Ehrke	ICT Governance, Risk and Compliance Manager	Daniel Ehrke	Feb 10, 2022	Daniel.Ehrke@transnet.net	084 445 6799
Group Risk	Virginia Dunjwa	GM: Group Enterprise Risk	Virginia Dunjwa (Feb 11, 2022 11:12 GMT+2)	Feb 11, 2022	Virginia.Dunjwa@transnet.net	060 847 1114
Compliance	Kgomotso Modise	GM: Group Compliance		Feb 23, 2022	Kgomotso.Modise@transnet.net	083 444 0047
Group Legal Services	Sue Albertyn	GM: Labour Law & Consequence Management	Sue Albertyn Sue Albertyn (Feb 23, 2022 14:45 GMT+2)	Feb 23, 2022	Sue.Albertyn@transnet.net	011 308 3630
Transnet Internal Audit	Busiwe Quma	GM: Technology and Technical Assurance – Internal Audit	n/a	n/a	Busiwe.quma@transnet.net	011 308 4501
Organised labour via Employee relations management	Neo Bodibe	GM: Employee Relations	Neo Bodibe (Apr 21, 2022 15:43 GMT+2)	Apr 21, 2022	Neo.Bodibe@transnet.net	083 762 0185

Recommended by Policy Owner and Policy Sponsor:

I hereby acknowledge that a search has been conducted and that the Policy is not duplicated or in conflict with any other Transnet Policies.

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Policy Owner	Stephen Mark	GM: Group Cyber Security, Governance, Risk and Compliance	Stephen Mark	Feb 10, 2022	Stephen.Mark@transnet.net	072 474 5597
Policy Sponsor	Pandelani Munyai	Group Chief Information Officer		10/5/2022	Pandelani.Munyai@transnet.net	064 809 9622

Group Executive Committee

Final Approval

23 June 2022

Date Signed Off

Summary of Version Control

Version Number	Effective Date	Summary of Changes
1.0	*November 2011*	*First release of the Policy.*
1.2	*August 2014*	*General updates to the Policy.*
1.3	*November 2014*	*Update headers and footers and corrected index numbers.*
2	*October 2015*	*General updates to the Policy.*
3	*January 2022*	*Formatting updated; content aligned with the latest ISO27001 standard.*

Contents

1 BACKGROUND

1.1. Transnet business relies on Information and Communications Technology (ICT) to provide an environment where business operations are executed in a smooth, un-interrupted and secure manner, while maintaining the confidentiality of information, such as financial information and operational procedures. At the same time, the current regulatory and legal frameworks place significant emphasis on the Information and Communications Technology Governance and specifically in the protection of information.

1.2. The Information Security Policy defines the approach and outlines the requirements that the Information Technology management must fulfil in order to provide business with a secure Information and Communication Technology (ICT) operations environment. The ICT Security policy is aligned to the ICT Governance Policy and the relationship is shown in Figure 1.

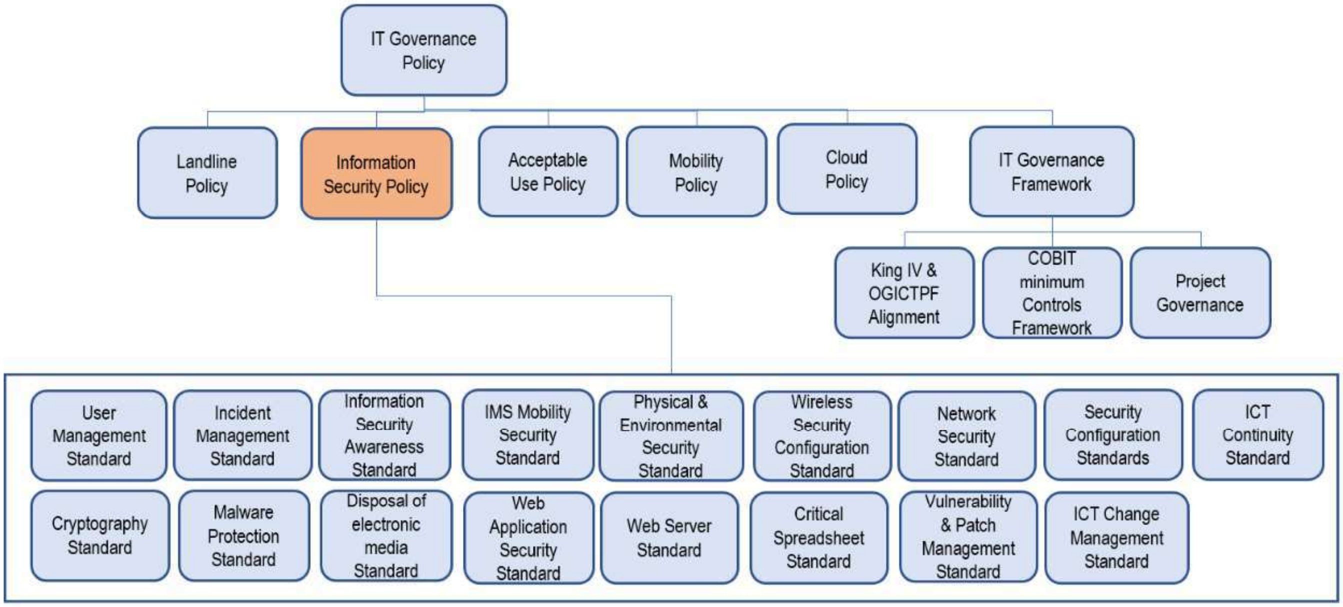

IT Governance Policy
Landline Policy
Information Security Policy
Acceptable Use Policy
Mobility Policy
Cloud Policy
IT Governance Framework
King IV & OGICTPF Alignment
COBIT minimum Controls Framework
Project Governance
User Management Standard
Incident Management Standard
Information Security Awareness Standard
IMS Mobility Security Standard
Physical & Environmental Security Standard
Wireless Security Configuration Standard
Network Security Standard
Security Configuration Standards
ICT Continuity Standard
Cryptography Standard
Malware Protection Standard
Disposal of electronic media Standard
Web Application Security Standard
Web Server Standard
Critical Spreadsheet Standard
Vulnerability & Patch Management Standard
ICT Change Management Standard

Figure 1

1.3. The Information Security Policy was developed and aligned to the ISO 27002 standard. The ISO 27002 standard is the code of practice for information security. It outlines potential controls and control mechanisms, which may be implemented.

1.4. The Information Security Policy establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management for the following areas (refer to figure 2):

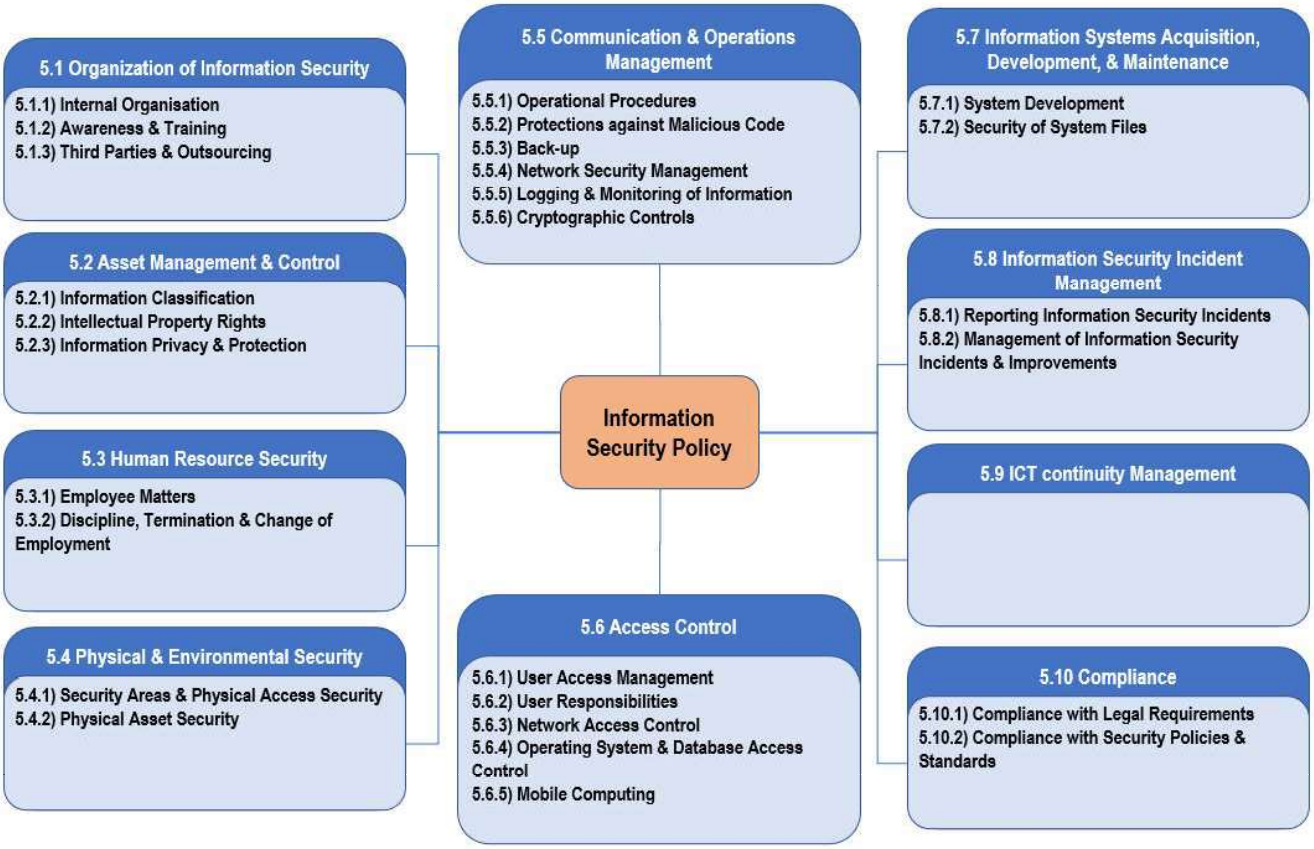

5.1 Organization of Information Security
5.1.1) Internal Organisation
5.1.2) Awareness & Training
5.1.3) Third Parties & Outsourcing
5.2 Asset Management & Control
5.2.1) Information Classification
5.2.2) Intellectual Property Rights
5.2.3) Information Privacy & Protection
5.3 Human Resource Security
5.3.1) Employee Matters
5.3.2) Discipline, Termination & Change of Employment
5.4 Physical & Environmental Security
5.4.1) Security Areas & Physical Access Security
5.4.2) Physical Asset Security
5.5 Communication & Operations Management
5.5.1) Operational Procedures
5.5.2) Protections against Malicious Code
5.5.3) Back-up
5.5.4) Network Security Management
5.5.5) Logging & Monitoring of Information
5.5.6) Cryptographic Controls
Information Security Policy
5.6 Access Control
5.6.1) User Access Management
5.6.2) User Responsibilities
5.6.3) Network Access Control
5.6.4) Operating System & Database Access Control
5.6.5) Mobile Computing
5.7 Information Systems Acquisition, Development, & Maintenance
5.7.1) System Development
5.7.2) Security of System Files
5.8 Information Security Incident Management
5.8.1) Reporting Information Security Incidents
5.8.2) Management of Information Security Incidents & Improvements
5.9 ICT continuity Management
5.10 Compliance
5.10.1) Compliance with Legal Requirements
5.10.2) Compliance with Security Policies & Standards

Figure 2 – Information Security Policy Areas

2 PURPOSE

2.1 The purpose of this policy is:

- Ensure compliance with current laws, and regulations,
- Ensure administrators and employees maintain the responsibility for ownership and knowledge about information security in order to minimise the risk of security incidents,
- Establish controls for protecting Transnet's information and information systems against abuse and other forms of harm or loss.

2.2 An Information Security policy statement expresses management's commitment to the implementation, maintenance, and improvement of its Information Security management system.

3 DEFINITIONS AND ABREVIATIONS

For ease of reference words, expressions and abbreviations used in the policy are defined below:

3.1 **Asset:** Any tangible or intangible object that has value to Transnet and includes, but is not limited to information, systems, facilities, networks, and computers.

3.2 **Business impact analysis (BIA):** The process by which the impact of a disaster or a business interruption on key business processes from both a quantitative and qualitative perspective are assessed, to include financial implications, performance impacts and any perceived impression on the brand or reputation of the organization. The BIA helps management decide for which business processes planning may be required and which continuity strategies to implement.

3.3 **Communication:** Includes both a direct communication and an indirect communication.

3.4 **Control:** Is any administrative, management, technical, or legal method that is used to manage risk. Controls are safeguards or countermeasures. Controls include practices, policies, procedures, programs, techniques, technologies, guidelines, and organisational structures. Controls can be deterrent, preventive, protective, detective, or corrective and typically are implemented to deal with a variety of root causes which result in risk.

3.5 **Cryptographic controls:** These are measures employed in the protection of information against unauthorised or unintentional disclosure and/or unauthorised alteration of the information.

3.6 **Demilitarised Zone:** Demilitarised zone is a sub-network (physical or logical) that contains a company's external services to a non-trusted network, such as the Internet.

3.7 **Direct communication:**

- Oral communication other than an indirect communication between two or more persons which occurs in the immediate presence of all the persons participating in that communication, or
- Utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who at the time that the indirect communication occurs is in the immediate presence of the person participating in the indirect communication.

3.8 **Employees:** means anyone who is on an indefinite contract of employment or on a fixed term contract or any person who works for Transnet, and who receives, or is entitled to receive remuneration, and any other person who in any manner assists in carrying on or conducting the business of Transnet, excluding independent contractors.

3.9 **Encryption:** Is the process of transforming readable information into something unreadable using an algorithm (or cipher) and a cryptographic key. The input into the process is often referred to as the plaintext and the output is known as the ciphertext.

3.10 **Entity:** Includes both individuals and processes.

3.11 **ICT:** Information and Communications Technology is the integration of telecommunications, computers, software, storage and systems that enable users to manipulate, transmit, access, and store information.

3.12 **ICT Continuity:** Capability of the organization to plan for and respond to incidents and disruptions in order to continue ICT services at an acceptable predefined level.

3.13 **ICT Continuity Plan/ Disaster Recovery Plan:** A written plan used to respond to the disruption of an organization's operations. This plan may focus on response to specific disruption scenarios.

3.14 **ICT Risk:** business risk associated with the use, ownership, operation, involvement, influence, and adoption of ICT within Transnet. It consists of ICT related events that could potentially impact the business considering both the likelihood and the impact of occurrence. It can occur with uncertain frequency and magnitude and it creates challenges in meeting strategic goals and objectives.

3.15 **IMEI:** International Mobile Equipment Identity, is a unique identification number assigned to identify devices with a sim card slot like mobile phones, tablets, or laptops. GSM networks use the IMEI number to identify and stop stolen devices from accessing the network.

3.16 **Indirect communication:** The transfer of information, including a message or any part of a message, whether:

- In the form of speech, music or other sounds, information, text, visual images (whether animated or not), signals or radio frequency spectrum, or
- In another form or in any combination of forms that is transmitted in whole or in part by means of a postal service or a telecommunication system.

3.17 **Information Asset:** Is information that has value to the extent that it enables Transnet to achieve business goals.

3.18 **Information:** The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical, or mechanical recording media.

3.19 **Information processing facility:** Any system, service, infrastructure, and the physical locations that house these.

3.20 **Information Resource:** The information and information assets of an organisation, department, or unit.

3.21 **Information Security events:** Indicates that the security of an information system, service, or network may have been breached or compromised. An Information Security event indicates that an Information Security policy may have been violated or a safeguard may have failed. This is a single event.

3.22 **Information Security incident:** Is made up of one or more unwanted or unexpected Information Security events that could potentially compromise the security of your information and weaken or impair your business operations.

3.23 **Information Security Management System (ISMS):** An Information Security Management System (ISMS) includes all of the policies, procedures, plans, processes, practices, roles, responsibilities, resources, and structures that are used to protect and preserve information. It includes all of the elements that organisations use to manage and control their Information Security risks. An ISMS is part of a larger management system.

3.24 **Information Security:** aims to achieve, maintain, and regulate appropriate levels of:

- **Confidentiality:** Ensuring that information is accessible only to those authorised to have access to the information and to ensure that it is not made available or disclosed to unauthorised entities,
- **Integrity:** Safeguarding the accuracy, unauthorised alteration and completeness of information and processing methods,
- **Availability:** Ensuring that authorised users have access to information and associated assets when required.

3.25 **Information System:** Is a system for generating, sending, receiving, storing, displaying, or otherwise processing information messages and includes the internet.

3.26 **Interception:** Means the aural or other acquisition of the contents of any communication through any means, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication and includes the:

- Monitoring of any such communication by means of a monitoring or interception device,
- Viewing, examination or inspection of the contents of any indirect communications,
- Diversion of any indirect communication from its intended destination to any other destination.

3.27 **ISGRC:** Information Security, Governance, Risk and Compliance.

3.28 **Keystroke Monitor:** A specialised form of interception software or hardware, that records every key stroke by a user and, possibly, every character of the response that returns to the user.

3.29 **Malicious Code:** Code, the execution of which may result in the loss of the integrity, confidentiality, or availability of information. Examples include, but are not limited to viruses, worms and trojan horses.

3.30 **Minimum Control Framework (MCF):** Is a selected subset of controls from the COBIT framework selected by EIMS in consultation with TIA.

3.31 **Mobile Code:** Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services.

3.32 **Mobile computing device administrator:** The appointed administrator/champion to manage mobile computing devices assigned to users.

3.33 **Mobile Devices or Mobile Computing and Storage Devices:** A portable device that allows people to work with information either locally or through a network connection. This includes, but is not limited to, notebooks, laptops, tablets, PDAs and smart phones. The definition excludes single purpose devices, such as hand-held terminals.

3.34 **Monitoring:** The method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of: user account logs, application logs, information backup and recovery logs, automated intrusion detection system logs, etc.

3.35 **Network Devices:** Network devices are components used to connect computers or other electronic devices together so that or that share files or resources such as printers

3.36 **Owner (Asset, Information, Information, Application):** Owners are formally responsible for making sure that assets / information / information / applications are secure while they are being developed, produced, maintained, and used.

3.37 **Platform:** A system on which application programs can run. Mobile phones running iOS, Symbian and Android are examples of platforms.

3.38 **Recovery Point Objective (RPO):** The recovery point objective of a set of information is the point in time to which the information must be restored for acceptable use of a system e.g. three days ago.

3.39 **Recovery Time Objective (RTO):** The timeframe that is available for the restoration of processes or service areas. Going beyond the RTO is the point at which a business is no longer viable.

3.40 **RICA:** The Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002.

3.41 **Sensitive Information:** Information which is currently not in the public domain. This information should be protected against unauthorised access or unwarranted disclosure. This would include the personal information of employees and commercially sensitive information.

3.42 **System Files:** System files refer to Operating System, database and application files that are important for the operation of an Operating System, database or application.

3.43 **Third party:** In the context of a specific issue, a third party is any person or body that is recognised as independent of the people directly involved with the application and implementation of this policy.

3.44 **Threat:** A threat is a potential unwanted event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organisation or system.

3.45 **TIA:** Transnet Internal Audit.

3.46 Transnet or “The Company” or “The Group”: Transnet SOC Ltd.

3.47 **Vulnerability:** Vulnerability is a weakness in an asset or group of assets. An asset's weakness could allow it to be exploited and harmed by one or more threats.

4 SCOPE

4.1 Information Security Policy covers the provision of organisational, technical and social measures necessary to safeguard information assets against unauthorised access, disclosure, denial of use, modification, diversion, destruction, loss, theft, or misuse, both malicious and accidental. The Information Security Policy jurisdiction covers all Transnet information assets (located at Transnet and non-Transnet locations) and begins with the electronic input of information and ends with its output using an electronic or non-electronic output medium.

4.2 The Information Security Policy applies to the Transnet Group and all Operating Divisions, including third parties servicing Transnet, employees, service providers and consultants.

5 POLICY STATEMENTS

5.1 ORGANISATION OF INFORMATION SECURITY

Internal Organisation

5.1.1.1 The Information Security Human Resources structure with detailed roles and responsibilities must be defined by the Information Security senior management.

Awareness and Training

5.1.1.2 An information awareness programme to promote compliance with information security regulations, policies and standards and promote protection of Transnet information assets, must be conducted by the Transnet ISGRC team annually.

Third Parties and Outsourcing

5.1.1.3 Third party access to Transnet information assets must be based on a formally executed contract. This contract must stipulate that all employees or agents of the third party are required to comply with all appropriate Transnet Information Security policy statements.

5.1.1.4 Prior to signing any ICT support agreement with a third party, the following requirements must be respected, and if necessary, included in the third-party contract:

- The definition of security administration, management, and control objectives,
- The separation of Transnet's and the third party's information, if on an external system the restrictions on copying information and securing assets,
- The right of Transnet to intercept Transnet communications must be in accordance with POPIA and RICA requirements,
- The requirement to prohibit access to Transnet information and systems without explicit authorisation from Transnet. and to maintain a list of individuals who have access to such information or system,
- The right of Transnet to monitor (and revoke) administrator rights,
- Facilities to rapidly disable any individual user ID,
- The responsibilities and procedures for reporting and handling security incidents,
- The right of Transnet to audit contractual responsibilities,
- The right of Transnet to perform on-site inspections of the information centre of external third parties.

5.1.1.5 The third party must ensure that all its employees and agents who have access to Transnet information are aware of and carry out their security responsibilities with respect to that information.

5.1.1.6 Third party access to Transnet information assets must be set to "no access" by default (i.e. all access rights must be explicitly granted). When granted, third party access to Transnet information assets must be for the minimum necessary period of time. Access to the assets must be approved by the asset owner(s) and the information process owner (if different from owner) or the GM: Cyber Security, Governance, Risk and Compliance.

5.1.1.7 Third party remote access to Transnet information assets will only be authorised in cases where there is a clearly defined business need. The access facility provided must limit the third party to the agreed method of access, the agreed access rights, and the agreed level of functionality.

5.1.1.8 Third party remote access to Transnet information assets must be approved by the asset owner(s) and the information process owner (if different from owner) or the Group CIO or GM: Cyber Security.

5.1.1.9 A regular review of all previously approved third party remote access must be conducted by the information owner. Any changes to the conditions upon which the third-party access was previously granted must be reviewed.

5.1.1.10 Prior to the implementation of a third-party remote access, the implementing party must request that an Information Security risk assessment be conducted by ISGRC and approved by the GM: Cyber Security, Governance, Risk and Compliance. to determine the necessary level of controls for that connection. All third-party connections must be classified according to the type of access required for the connection, thereby identifying the necessary security controls required for the connection approval.

5.1.1.11 When third party access needs to be granted with system-level privileges (e.g. root or supervisor level access), such rights must be granted for a limited duration, and de-activated when not required. The access usage must be subject to supervision and must be fully logged.

5.1.1.12 The third party must comply with all Transnet Information Security policies, standards and procedures. information assets that have been entrusted to a third party must only be used by the third party for the purposes agreed. Transnet information must not be disclosed to any non-Transnet party for any purpose other than the one that has been expressly authorised by Transnet.

5.1.1.13 Third party access to Transnet information assets, and in particular, access to customer information must be in accordance with legal and regulatory requirements for trade and business secrecy and information protection.

5.1.1.14 A risk assessment must be carried out by the ISGRC team and approved by the GM: Cyber Security before considering the outsourcing of an information service.

5.1.1.15 Third party contracts must include controls for the protection of sensitive information.

5.1.1.16 Local laws must always be considered prior to outsourcing services or storing information in cross border locations. Unless the local laws at the outsourcing location can guarantee adequate protection of the information, outsourcing cross national borders is not permitted.

5.1.1.17 Contracts must always give Transnet the right to audit the service provider to ensure compliance with the contractual requirements.

5.2 ASSET MANAGEMENT AND CONTROL

Information Classification

5.2.1.1 Information must be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation in accordance with Transnet's Information Classification Policy. The minimum requirement for protecting the confidentiality of all information regardless of classification is the application of access control and authorisation.

5.2.1.2 All information removed from the Transnet premises, for offsite backup reasons or the repair of hardware devices (PC's, servers), must be adequately secured and controlled before the release of the information from the premises.

5.2.1.3 All sensitive information must be properly deleted from the media, including backups, with no residue remaining that could be recovered by unauthorised individuals.

Intellectual Property Rights

5.2.1.4 Without specific written exceptions, all programs and documentation generated by personnel for the benefit of Transnet are the property of Transnet. All computer programs and documentation owned by Transnet must include appropriate copyright notices.

5.2.1.5 All software on Transnet computers is protected by copyright laws. Commercial software purchased by Transnet is authorised for Transnet use only and must be utilised in accordance with contractual agreements and copyright laws. Unless specifically authorised within the license agreement, making copies of copyrighted software for personal use is prohibited.

5.2.1.6 Transnet strongly supports strict adherence to software vendor license agreements and copyright holder notices. Whenever bundled systems are being procured, the source must provide written evidence of the software licenses. The agreements for all computer programs licensed from third parties must be periodically reviewed for compliance and additional licensed copies procured as required.

5.2.1.7 Transnet critical hardware and software products must be registered with the appropriate vendors to assure that support and upgrades are readily available.

5.2.1.8 Transnet information, computer software and other information assets must be used for authorised business purposes.

Information Privacy and Protection

5.2.1.9 Transnet employees must ensure that personal information stored in Transnet devices is secured and protected. Transnet makes all reasonable efforts to respect the privacy of information stored on Transnet information assets.

5.2.1.10 Transnet reserves the right to have authorised personnel intercept information at the user level or user communications in the best interests of Transnet or in contravention of Transnet policies. This will be conducted in compliance with requirements specified by POPIA and RICA.

5.3 HUMAN RESOURCES SECURITY

Employee Matters

5.3.1.1 Transnet employees, contractors and third-party users / vendors must act in accordance with Transnet's Information Security Policy and accompanying standards, guidelines and procedures.

5.3.1.2 Individuals in the possession of portable laptops, notebooks, smartphones, tablets, and other transportable computers or storage media (such as USB devices) containing Transnet information must not leave these unattended at any time unless the device and information has been properly safeguarded. Such individuals take full responsibility for the equipment and the information it retains.

Discipline, Termination and Change of Employment

5.3.1.3 In all cases, where employees terminate their employment with Transnet, they must return all Transnet equipment and information back to Transnet.

5.3.1.4 Upon the termination or expiration of their contract, all contractors, consultants, and temporary staff must relinquish all copies of Transnet information received or created during the performance of the contract.

5.3.1.5 The access rights of the above parties to Transnet information and information processing facilities must be removed upon termination of their employment, contract or agreement.

5.4 PHYSICAL AND ENVIRONMENTAL SECURITY

Secure Areas and Physical Access Security

5.4.1.1 Buildings that house Transnet computers or communications systems must be protected with physical security measures that prevent unauthorised persons from gaining access.

5.4.1.2 To ensure that only authorised personnel are allowed access, security perimeters such as walls, card controlled entry gates or manned reception desks must be used to protect areas that contain information and information processing facilities.

5.4.1.3 Printers used for printing confidential information must not be left unattended if they are located in an open environment. Secure printing must be used whenever supported by a printer. Printed material must be appropriately handled and protected by the person that printed them.

5.4.1.4 Access to Transnet information equipment by hardware maintenance staff must be controlled. This includes proper staff identification, logging of work done, and supervision to ensure that no unauthorised modifications are performed on any equipment other than that which is to be maintained.

Physical Asset Security

5.4.1.5 Transnet premises for information equipment must meet minimum environmental standards for power, cooling, humidity, etc. as per supplier recommendations to ensure continued availability and integrity.

5.4.1.6 The security requirements for equipment stored off-site must be the same as the requirements for on-site equipment.

5.4.1.7 Network control devices, diagnostic equipment, security firewall systems and encryption key management systems must be stored in physically secure locations.

5.4.1.8 All storage media must be disposed of as per the "Disposal of electronic Storage Media Standard".

5.4.1.9 During extended periods away from your desk, sensitive working documents must be placed in a securely locked area such as a locked drawer.

5.4.1.10 Employees must place all office documents in securely locked desks or cabinets at the end of the day.

5.4.1.11 Theft or loss of a Transnet asset must be reported to the Security department for investigation. The Security department is responsible managing access to Transnet physical facilities.

5.4.1.12 The owner or official user of the asset lost must report the incident to the South African Police Services (SAPS) and where applicable, the relevant service providers.

5.5 COMMUNICATIONS AND OPERATIONS MANAGEMENT

Operational Procedures

5.5.1.1 The following operational procedures exist as a minimum for all systems:

5.5.1.1.1 Logical access must be managed in a standardised manner in accordance with the requirements outlined in the "User Management Standard".

5.5.1.1.2 Operating procedures must be documented, maintained and available for information technology processes as necessary.

Protection against Malicious Code

5.5.1.2 Detection, prevention and recovery controls must be implemented to protect the Transnet Information Technology resources against malicious code.

Back-up

5.5.1.3 Backups must be performed as per documented schedules, monitored and stored off-site in secured locations.

5.5.1.4 Back-up copies of information and software must be protected at the same levels of security as the original information. Back-up copies of information and software must be restored for testing purposes on a periodic basis.

5.5.1.5 Backups of business information must be done on the business servers not on desktops.

Network Security Management

5.5.1.6 Network devices must be secured, managed and monitored by senior management to protect the devices and the information transmitted through them.

Logging and Monitoring of information

5.5.1.7 Auditing must be enabled on all systems at all times in accordance with the Minimum Control Framework.

5.5.1.8 Additional audit logs must be enabled to accommodate business or security requirements as per the application / information owner request and in accordance with the classification level of the information.

5.5.1.9 Audit logs must have the capability to be reviewed for identification of exceptions and are kept for a defined period of time in support of the review cycles.

5.5.1.10 Controls must be in place to protect the logging facilities and the information logged against tampering and unauthorised access.

5.5.1.11 The clocks of all the Transnet information processing systems must be synchronised with a NTP time source to ensure consistent time stamping of logs.

5.5.1.12 All technologies implemented in the Transnet environment must have a Minimum Security Baseline Standard.

Cryptographic Controls

5.5.1.13 Information must be encrypted in storage and in transit as per the requirements outlined in the "Information Classification Policy" for the respective level of classification.

5.6 ACCESS CONTROL

User Access Management

5.6.1.1 Access to applications, systems and resources must be granted in accordance with the relevant authorised job description profile.

5.6.1.2 User accounts and assigned privileges must be regularly reviewed by the information asset owner to ensure the validity of the user accounts, the segregation of duties and the appropriateness of the privileges assigned to the users.

User Responsibilities

5.6.1.3 Users must be reminded of their responsibility to comply with security policies and standards when they request or change access by submitting an Access Form.

5.6.1.4 Employees must not be allowed to intercept any information without authority or permission as doing so is an offence and may be prosecuted as per RICA.

Network Access Control

5.6.1.5 The capability of users to connect to the network and use network services must be restricted according to the job description profile of each user.

5.6.1.6 Ports services and similar facilities installed on a computer or network resources must be disabled or removed unless required for business purposes.

Operating System and Database Access Control

5.6.1.7 Access to the operating systems and databases must be configured securely. Logical access controls must be implemented to allow appropriate identification and authentication of users in order to limit the access exposure of the resources and the information stored in or processed by them.

5.6.1.8 Logical access management controls, including account and password controls must be implemented as per the "User Management Standard".

Mobile computing

5.6.1.9 Controls must be implemented to ensure the secure access to information on devices used for mobile computing. Such devices include smartphones, laptops, notebooks, and other portable computers. Users may bring their own devices into the Transnet environment subject to complying with all the security requirements applicable to Transnet owned equipment.

5.7 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

System Development

5.7.1.1 Information Security must be considered at all stages of the system development life cycle.

5.7.1.2 Transnet information systems must comply with all relevant Information Security policies, directives, standards, procedures and legal documents consistent with the business needs of Transnet.

5.7.1.3 A Transnet approved risk assessment methodology must be used to help ensure that appropriate Information Security controls are designed and built into new systems from the beginning.

5.7.1.4 Security mechanisms must be made available as modules that are technically separated from applications and that conform to internationally accepted standards wherever possible.

5.7.1.5 The technical and organisational binding of security services into applications must be based on standardised interfaces and processes.

5.7.1.6 Development staff must document all aspects of how Information Security has been considered and implemented at all stages of the software development life cycle (SDLC). When first published, such documentation must be issued to and approved by the Information Risk Security Governance and Compliance Steering Committee.

5.7.1.7 Developers must be responsible for the design and implementation of tests to ensure that Information Security controls meet previously specified acceptance criteria. The tests must be completed prior to production implementation.

5.7.1.8 The use of production information for development testing is prohibited. Information used for testing must be desensitised and approved by the information owner prior to release, use of desensitised production information must never jeopardise security or business-related privacy.

5.7.1.9 Business application systems must go into production when all users and information operations staff have received appropriate documentation and training in such issues as: how security incidents are handled, how emergency support access for developers is managed, and what users must do if they forget their password.

5.7.1.10 The ISGRC Steering Committee must confirm their approval that a new system satisfies all necessary security requirements prior to that system being used in a Transnet production environment.

5.7.1.11 Prior to moving software and/or system to production status, all special access paths must be removed so that access may only be obtained via normal secured channels.

5.7.1.12 The development environment must be physically or logically separate from the production environment. The development staff must not have access to production systems. The development staff may be granted access where appropriate lo their function for a limited period of time for essential support purposes.

5.7.1.13 All third party developed products used within Transnet must comply with Information Security policies, procedures, standards, etc. The installing agency must verify this compliance before the third party product is installed in Transnet.

5.7.1.14 A third party software product must be able to be integrated with the existing security system(s). of blocking unauthorised access to programs, functions, and information.

5.7.1.15 Standard procedures must be followed both for the tests and for the introduction of the third party software product into production.

5.7.1.16 System and information owners must be allocated prior to the implementation and go-live of a system.

5.7.1.17 Access to source code must be restricted to the relevant developers on the development environment and only production applications are installed on the production systems.

Security of System Files

5.7.1.18 Access to system or application sensitive files must be restricted to appropriate system users and is in accordance with the user's job function.

5.8 INFORMATION SECURITY INCIDENT MANAGEMENT

Reporting Information Security incidents

5.8.1.1 All employees, contractors and third party users of information systems and services must report security incidents to the Transnet Helpdesk.

Management of Information Security Incidents and Improvements

5.8.1.2 Reports of the incidents from the Helpdesk must be made available to the Information Risk Security Governance and Compliance Steering Committee (ISGRC-SSC) and must be used to identify trends or recurring incidents.

5.9 ICT CONTINUITY MANAGEMENT

5.9.1 ICT Continuity management must be a collaborative effort of the OD Heads of ICT and the Group CIO.

5.9.2 An ICT Continuity Programme must be developed and implemented for all Operating Division functions and EIMS functions to maintain essential customer services and critical business processes.

5.9.3 The ICT Continuity Programme must align with the Transnet Business Continuity management policy.

5.9.4 ICT continuity strategies must be developed based on the results of a formal a business impact assessment (BIA}.

5.9.5 ICT risk assessments (RA) must be conducted in line with the Transnet ICT Risk Management Framework including the continuity risks in the ICT Risk Universe.

5.9.6 The ICT continuity, processes standards and guidelines. must be reviewed, tested and updated every two years or after significant changes in order to verify that continuity objectives are achievable.

5.9.7 The ICT continuity plans. procedures and arrangements must be reviewed, tested and updated bi-annually or after significant changes in order to verify that continuity objectives are achievable.

5.9.8 An ICT continuity education programme must be established and maintained to ensure that all Transnet IMS employees that are responsible for ICT continuity are adequately and continuously trained. The training must enable the IMS employees to perform their required tasks competently.

5.9.9 An ICT continuity awareness programme must be established and maintained to ensure that ICT enabled Transnet employees are aware of ICT continuity arrangements and their roles, and responsibilities within the programme.

5.10 COMPLIANCE

<u>Compliance with Legal Requirements</u>

5.10.1.1 The developers of Information Security policies and standards must compile or update the respective documentation in-line with the legal and regulatory requirements outlined in the "Transnet Regulatory Universe". The regulatory requirements that affect Information Security are listed in section "Related Information and Reference" of the current document.

Compliance with Security Policies and Standards

5.10.1.2 Controls must be implemented to ensure compliance with the requirements set in the Information Security Policy and the supporting Standards. The controls must be documented and operated effectively and must cater adequately for deviations from technical standards in a manner which does not introduce risk to the business.

6 ROLES AND RESPONSIBILITIES

6.1 GM: ISGRC (CYBER SECURITY, GOVERNANCE, RISK AND COMPLIANCE)

6.1.1 Ensure security assessments of Information Security platforms are performed prior to those being approved. The platforms must conform to the Transnet security requirements.

6.1.2 Ensure that security configuration standards are defined and implemented for all platforms used to access or store Transnet information.

6.2 GROUP ISGRC STEERING COMMITTEE

The members of the committee must:

6.2.1 Participate in the development and maintenance of the Transnet Information Security Policy and the supporting standards,

6.2.2 Facilitate the deployment of the Transnet Information Security Policy to all Operating Division,

6.2.3 Monitor that all Operating Division ICT Departments complies with the Policy and report non-compliance.

Information Security Policy RACI

6.2.3.1 **Accountable:** Group Chief Information Officer and Senior Management.

6.2.3.2 **Responsible**: GM: Cyber Security, Governance, Risk and Compliance.

6.2.3.3 **Informed:** Operating Division's CIO.

6.2.3.4 **Support:** Group ICT.

6.2.3.5 **Monitoring and maintenance:** Information Security.

7 RELATED INFORMATION AND REFERENCE

This policy should be read in conjunction with the following documents, Policies and regulatory requirements:

7.1 INTERNAL DOCUMENTS:

7.1.1 Transnet Acceptable Use Policy,
7.1.2 Transnet Disposal of Electronic Storage Media Standard,
7.1.3 Transnet User Management Standard,
7.1.4 Transnet Register of Approved Mobile Platforms,
7.1.5 Transnet Cellular Procedures Document,
7.1.6 Transnet Records Management Policy,
7.1.7 Transnet Information Classification Policy,
7.1.8 Transnet Information Classification Standard,
7.1.9 Transnet Physical Environmental Standard,
7.1.10 Transnet Security configuration Standards,
7.1.11 Transnet Regulatory Universe,
7.1.12 Transnet Disciplinary Code and Procedures Policy.

7.2 EXTERNAL DOCUMENTS:

7.2.1 Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002) (RICA),
7.2.2 The Protection of Personal Information Act, 2013 (Act No 4 of 2013),
7.2.3 Electronic Communications and Transactions Act (Act No. 25 of 2002),
7.2.4 ISO 27001/2 (Information Security Management System and controls),
7.2.5 ISO 27031 (Guidelines for information and communications technology readiness for Business Continuity),
7.2.6 Copyright Act No 98 of 1978,
7.2.7 Intellectual Property Laws Rationalisation Act No.107 of 1996,
7.2.8 Promotion of Access to Information (Act 2 of 2000),
7.2.9 King IV Code on Corporate Governance,
7.2.10 Cybercrimes Act (Act no. 19 of 2020).

8 FINANCIAL IMPLICATIONS

8.1 Budget provision for the implementation of the policy should be allocated according to the cost centre management procedures.

9 EXCLUSIONS

9.1 There are no exclusions to this Policy.

10 REQUEST TO DEVIATE FROM POLICY

10.1 In cases where material and compelling circumstances merit deviation(s) from particular provision(s) of this policy, written submissions shall be submitted to the Group Cyber Security GM, who shall have full authority to grant such request, in whole or in part, or to refuse same.

10.2 Exceptions will only be allowed following a risk assessment and a signed risk acceptance from the Line Manager of the user. Thereafter, a waiver will be issued by the GM: Cyber Security, Governance, Risk and Compliance.

10.3 The exception will be granted for a maximum of six months and will have to be reviewed every six months if it is still required.

11 NON-COMPLIANCE

11.1 Breaches of this policy will be viewed in a very serious light. Employees who do not conform to this Policy or Principles and Standards may be subject to disciplinary action in terms of the applicable Transnet disciplinary processes and procedures.

11.2 Each Operation Division is responsible for ensuring compliance to the principles/rules of this Policy.

TRANSNET

delivering freight reliably

Transnet Cloud Standard

Version Number	*V1.0*
Next Review Date	*2 years from the final approval date*
Standard Owner	*Mark Snyders: GM Technology Innovation & Digital Transformation*
Signature	Mark A Snyders
Standard Sponsor	*Pandelani Munyai: Group Chief Information Officer*
Signature	
Date Approved	3 June 2024

Approved by:

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Subject Matter Expert	Shawn Norton	Snr Manager: Group ICT Infrastructure	Norton	May 31, 2024	Shawn.Norton@transnet.net	083 795 1575
Subject Matter Expert	Sibusiso Mthimunye	Cyber Security Specialist	Sibusiso Mthimunye (May 30, 2024 12:27 GMT+2)	May 30, 2024	Sibusiso.Mthimunye@transnet.net	084 245 7086

I hereby acknowledge that a search has been conducted and that the Standard is not duplicated or in conflict with any other Transnet Standards.

	Name	Designation	Approval Signature	Date	E-Mail	Contact Number
Owner	Mark Snyders	GM Technology Innovation & Digital Transformation	Mark J Snyders	May 30, 2024	Mark.Snyders@transnet.net	083 308 6550
Sponsor	Pandelani Munyai	Group Chief Information Officer			Pandelani.Munyai@transnet.net	011 308 3071

Final Approval

RRThipe

ICT Architecture Review Council

16.09.2024

Date Approved

Summary of Version Control

Version Number	Effective Date	Summary of Changes
1.0	*November 2018*	- *Initial Cloud Policy*
1.0	*May 2024*	- *Initial Cloud Standard*

Table of Contents

1. INTRODUCTION

This Cloud Standard sets out the rules by which decisions to consume cloud services must be made and managed in Transnet. Transnet has clear set of objectives as articulated in its strategy, currently the Shareholder Compact, Corporate plan, and all applicable Governance structures. It is also Transnet's objective to accelerate the digital roadmap which has cloud-based technologies as one of the critical enabling blocks. The era of sensor technologies, predictive capabilities and Internet of Things has led to "Big Data" requiring increased processing power and consumptive models of IT. With the physical world forming part of the enterprise so rapidly, Transnet is facing serious challenges and if these are not addressed by adaptation then we face extinction. Smart consumption of IT as a commodity is now critical not only for IT, but for business as well.

Transnet is putting into place the standard, skills, and tools necessary to accelerate the adoption of cloud and to become less technology-centric and more outcome-focused.

Through this standard, Transnet endorses the use of cloud services in enabling its operations. The standard further provides guidelines in the use of cloud services for Software as A Service (SaaS), Platform as a Service (PaaS), and all other "XaaS" with respect to access, management, and protection of data for all its stakeholders:

- Vendors.
- Transnet contractors.
- Transnet employees.
- Transnet partners.
- Transnet clients when interacting or who can provide appropriate levels of protection and recovery for Transnet's information.

While cloud storage of files can expedite collaboration and sharing of information anytime, anywhere, and with anyone, there are some guidelines that must be in place for the kind and type of internal information that is appropriate for storing and sharing using these services.

2. PURPOSE

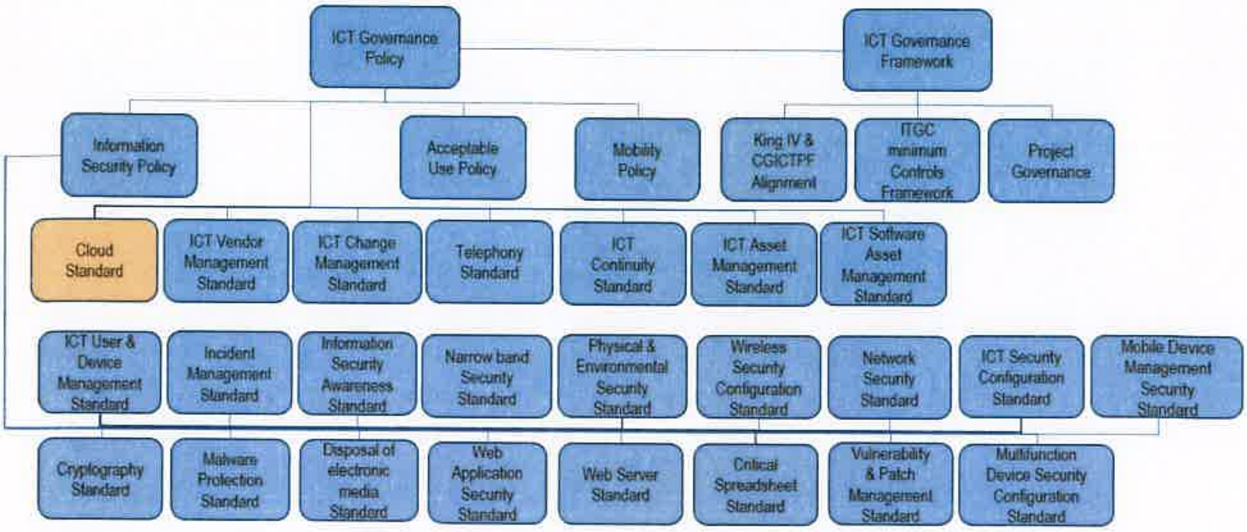
This Standard identifies the minimum baseline configuration and security requirements and provides related 'good practice' for effective and efficient management of the Cloud computing environment within Transnet.

With the modernisation and transformation of the Transnet IT installed base, commoditising IT moves to the centre to enable agility, speed of processing and speed of response. This modernisation will also make Transnet a critical player in the Transport and Logistics industry not only in South Africa, but globally.

It is also the purpose of this standard to encourage consumption of cloud-based services by all Transnet stakeholders within a secure environment. The intention is to move away from unnecessary ownership of ICT infrastructure and let Transnet consume it on a usage basis where appropriate.

Within the context of the Transnet Information Security Management System (ISMS), The Cloud Standard supports the ICT Governance Policy and the ICT Governance Framework as depicted below:

ICT Policies, Standards & Frameworks


ICT Governance Policy
ICT Governance Framework
Information Security Policy
Acceptable Use Policy
Mobility Policy
King IV & CGICTPF Alignment
ITGC minimum Controls Framework
Project Governance
Cloud Standard
ICT Vendor Management Standard
ICT Change Management Standard
Telephony Standard
ICT Continuity Standard
ICT Asset Management Standard
ICT Software Asset Management Standard
ICT User & Device Management Standard
Incident Management Standard
Information Security Awareness Standard
Narrow band Security Standard
Physical & Environmental Security Standard
Wireless Security Configuration Standard
Network Security Standard
ICT Security Configuration Standard
Mobile Device Management Security Standard
Cryptography Standard
Malware Protection Standard
Disposal of electronic media Standard
Web Application Security Standard
Web Server Standard
Critical Spreadsheet Standard
Vulnerability & Patch Management Standard
Multifunction Device Security Configuration Standard

3. SCOPE

This standard applies to all Transnet systems deployed within cloud environments. This standard also applies to all system owners and custodians where applicable. Any cloud-based solution must, at minimum meet the requirements in this standard. There are cloud-based solutions available that are not able to have certain elements of this standard applied, in which case they will be evaluated at the design stage at which point, exemption may be sought from the relevant Governance Committee(s).

This standard pertains to all external cloud services, e.g., cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Management-as-a-Service (MaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact your ICT team.

4. DEFINITIONS AND ABBREVIATIONS

For ease of reference words, expressions and abbreviations used in the standard are defined below.

Azure Fabric: Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers.

CGICTPF: Corporate Governance of Information and Communications Technology Policy Framework. DPSA framework instituted by cabinet. December 2013. Transnet falls within the scope of the framework for implementation as a state-owned entity.

Cloud (Definition of cloud from NIST): Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing: Is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, Transnet for services such as, but not limited to, social networking applications (e.g., blogs and wikis), file storage (Drop Box), and content hosting (publishers textbook add-ons).

CMDB: Configuration Management Database is an ITIL term for a database used by an organization to store information about hardware and software assets (commonly referred to as configuration items).

DOA: Delegation of Authority provides Signature Authority to certain individuals based on their level in the organization to approve various transactions.

DPSA: Department of Public Service and Administration.

GICTF: Governance of ICT Framework. An abstraction that defines the elements for the effective and efficient directing and controlling of ICT resources to facilitate the achievement of company strategic objectives.

ICT: Information and Communications Technology.

Infrastructure as code (IaC): Is the managing and provisioning of infrastructure through code instead of through manual processes.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

ISO 27001: Is an international standard to manage information security.

IT and Digital Governance Framework - An abstraction that defines the elements that support the effective and efficient directing and controlling of ICT resources (people, process, and technology) to facilitate the achievement of Transnet's strategic objectives.

MaaS (Management as a Service): Cloud-based service model that provides businesses with outsourced management solutions for various aspects of their operations. MaaS involves the delegation of tasks related to IT infrastructure, applications, security, or other business processes to a third-party service provider. E.g., Software managed for Transnet with Transnet specific configuration requirements.

NIST: The National Institute of Standards and Technology is an agency of the United States Department of Commerce whose mission is to promote American innovation and industrial competitiveness.

OMS: Operations Management Suite (OMS) is an advanced, comprehensive offering that brings together four complementary Azure services: Backup, Site Recovery, Log Analytics and Automation and is one of the tools Microsoft leverages when providing managed Azure consulting services.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Portability- The ability to transfer data from one system to another without being required to recreate or re-enter data descriptions or to modify significantly the application being transported. 2. The ability of software or of a system to run on more than one type or size of computer under more than one operating system. 3. Of equipment, the quality of being able to function normally while being conveyed. (Source: NIST Cloud Taxonomy)

Private Cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. (Source: NIST Cloud Taxonomy) It is a Cloud ecosystem or platform specifically for an organisation with its own rules and governance and for its own consumption only. The platform is not a shared platform and can be across multiple cloud providers. The classification of data will be according to data classification policies i.e., which data is for public consumption, and which is for Private Consumption.

Probity - Strict adherence to a code of ethics based on undeviating honesty, especially in commercial (monetary) matters and beyond legal requirements.

Public Cloud - The cloud infrastructure is made available to the public or a large industry group and is owned by an organization selling cloud services. (Source: NIST Cloud Taxonomy)

Regulatory Requirements -Any legislation applicable to Transnet, i.e., legislation as set out in the Transnet Regulatory Universe as amended from time to time. e.g., National Treasury Regulations and the Public Finance Management Act No 1 of 1999 (PFMA).

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

Terraform: Terraform uses declarative syntax to describe your Oracle Cloud Infrastructure (OCI) infrastructure and then persist it in configuration files that can be shared, reviewed, edited, versioned, preserved, and reused.

TCP / UDP: Transmission Control Protocol (TCP) / User Datagram Protocol (UDP).

Transnet: "The Company" or "The Group" - Transnet SOC Ltd.

5. ROLES AND RESPONSIBILITIES

5.1. ICT Architecture Review Council

- Responsible for the final approval of all Transnet ICT Standards.
- Responsible for providing approval for any new cloud deployments.

5.2. GM: Technology Innovation & Digital Transformation

- Owner of the standard.
- Responsible for overseeing the development, enforcement, and measurement of this standard.
- Reviews and supports waivers that have been compiled for exception from compliance with this standard.
- Overall accountability for overseeing assurance reviews to ensure compliance with this standard.

5.3. Information Security, Governance, Risk and Compliance Committee

- Responsible to manage and co-ordinate ICT risk mitigation and governance activities across the Group and to co-ordinate activities regarding the protection of Transnet's information assets.
- Participate in the development and maintenance of the standard and/or related processes.
- The committee is responsible for recommending Transnet ICT standards to the ICT Architecture Review Council for final approval.
- ISGRC committee members participate in the development and maintenance of the standard and the related procedures.
- Report compliance to the GM: Technology Innovation & Digital Transformation.

5.4. GM: Enterprise Technology Services

- Ensure the standard is communicated to all parties (including third parties) that are responsible for designing, developing, and managing web-based applications in the Transnet environment.
- Ensure implementation of this standard.

5.5. Operating Division Information Security Liaison

- Facilitate the implementation of the standard in the OD by communicating the requirements, providing technical assistance with implementation, and reporting adherence to the standard.
- Co-ordinate the compliance with this standard.

5.6. Vendor Manager

- Ensure that compliance requirements for this standard are included in vendor/supplier contracts and requirements of any engagement that involves the design, development and/or implementation of web applications.

5.7. Transnet Operating Division ICT

- Communicate requirements of the standard to all ICT departments and relevant third parties.
- Establish mechanisms and controls to ensure compliance to this standard within your respective operating division.
- Participate in the on-going maintenance, review, and enhancement of this standard.

5.8. Vendors, Third-Party Suppliers System Owners/Custodians

- Ensure that the requirements of this standard are formally adopted and enforced during the design, acquisition, implementation, or deployment of computer/information systems in the Transnet environment.

5.9. Transnet Group Change Advisory Board (CAB)

- Responsible for providing final approval for any new or changes to cloud deployments.

6. REQUIREMENTS

The following stipulations must be complied with to ensure that Transnet Cloud services are efficiently managed:

6.1. GENERAL:

6.1.1. Cloud based solutions and services will be the first consideration for Transnet when new applications or solutions are considered.

6.1.2. The consumption of Public Cloud solutions must comply with the principle of portability as defined in this standard and be in line with both the letter and spirit of this standard.

6.1.3. A business case for cloud based versus on premise solutions must be completed each time a new solution is considered.

6.1.4. For all cloud-based solutions, there must be a clear and approved DR (Disaster Recovery), back up procedures and standards and integration requirements if any. Ease of integration with core systems must be assured.

6.2. COST MANAGEMENT:

Cost management for Cloud managed Services	
Justification / Description	The effectiveness of Cost Management depends on the controls implemented to mitigate associated risks. Below are the controls that must be complied with to ensure effective cost management.
Standard Requirements	The following requirements must be complied with: **6.2.1. <u>Cloud Procurement:</u>** Any end user, working group, or department looking to use cloud services for either single project based work or ongoing work, must ensure that: **6.2.1.1.** In situations where cloud service providers have pre-drafted contracts, these must be reviewed by the relevant Transnet's legal department in consultation with the ICT department prior to these being accepted. **6.2.1.2.** For any cloud services that require individual users to agree to terms of service or usage, the office of the relevant Transnet's legal department in consultation with the ICT department will review such documents and determine if end users can agree on an

	individual basis or identify any needed changes. This is to mitigate the risk that employees may inadvertently bind Transnet by simply clicking "Yes", "Okay", "Accept" without realising that there is an underlying contract that may bind Transnet. **6.2.1.3.** Any usage of cloud services must include a Disaster Recovery and Business Continuity capabilities where in the event of a data disaster Transnet is able to recover any lost data. **6.2.1.4.** All Transnet RFS's (Request for Services) for cloud-based services will be written in line with this standard. **6.2.1.5.** The contract must specifically state what data Transnet owns. It must also classify the type of data shared in the contract according to the Transnet's classification policy. **6.2.1.6.** The contract must specify how the cloud-computing vendor can use Transnet's data. Vendors cannot use Transnet's data in any way that contravenes South African law or infringe on Transnet data ownership rights. **6.2.1.7.** IT-related risks must be identified, recorded, evaluated, mitigated, and monitored, and reported in accordance with the approved Transnet ERM (Enterprise Risk Management) framework and policy. **6.2.1.8.** Without compromising the Transnet Supply Chain policies and procedures, all information technology acquisition activities, including hardware, software, telecom, and professional services, must be managed through the appropriate ICT governance structures and in line with the Transnet Delegation Framework. **6.2.1.9.** Heads of ICT must establish formal processes for ICT value optimisation to continually evaluate the portfolio of ICT- enabled investments, direct value management principles and practices and monitor key goals and metrics. **6.2.1.10.** As a transition, any cloud solution currently deployed will be deemed to comply with this standard but will be assessed by the relevant CIO to determine if it materially complies with this standard. If after such an assessment is done it is determined that the solution does not comply, cost effective mitigation actions will be undertaken to address the said non-compliance. **6.2.1.11.** There must be a clearly documented exit plan i.e., timelines, cost and approved procedures for all cloud-based solutions and services. This is in effect, to secure Transnet's ability to continue operations in the event a cloud service provider is unable to provide service, or the service level is no longer acceptable to Transnet. The exit plan must form part of the contract specifying the format in which data must be returned and the process of how data will be securely deleted.

6.2.2. **Resource Cost Management:**

Any end user, working group, or department looking to use cloud services for either single project based work or ongoing work, must ensure that:

6.2.2.1. A multi-disciplinary cloud cost management team must be established and tasked with oversight and implementation of cost-related strategies.

6.2.2.2. Cost optimisation KPIs must be developed and tracked.

6.2.2.3. Start and stop of workloads during times when not required (e.g., December holidays / quiet periods) must be configured.

6.2.2.4. Implement auto-scaling to dynamically adjust resource capacity based on workload fluctuations, ensuring optimal performance while minimizing costs during off-peak hours.

6.2.2.5. Regularly review and optimize the allocation of cloud resources to ensure they are appropriately sized for the workload demands, thus avoiding over-provisioning and unnecessary costs. (Resource Right-Sizing).

6.2.2.6. Implement monitoring controls on resource utilization to identify underutilized or idle resources, allowing for timely decommissioning or downsizing to prevent unnecessary expenditure.

6.2.2.7. Utilize reserved instances or savings plans for predictable workloads to benefit from discounted pricing compared to on-demand usage (Reserved Instances and Savings Plans).

6.2.2.8. Leverage spot instances or low-priority virtual machines for non-critical, fault-tolerant workloads to take advantage of cost savings during periods of low demand (Spot Instances and Low-Priority VMs).

	6.2.2.9. Establish lifecycle policies to automatically archive or delete unused resources, such as snapshots, storage, and temporary instances, to prevent unnecessary storage costs (Lifecycle Management). **6.2.2.10.** Enforce tagging standards to categorize resources by owner, department, project, or environment, enabling accurate cost allocation and facilitating cost accountability (Tagging and Cost Allocation). **6.2.2.11.** Set up cost alerts and budgets to notify stakeholders when spending exceeds predefined thresholds, enabling proactive cost management and preventing budget overruns (Cost Alerts and Budgets). **6.2.2.12.** Implement storage optimization such as tiered storage, data compression, and deduplication, to minimize storage costs while maintaining data accessibility and performance (Optimized Storage Solutions). **6.2.2.13.** Foster a culture of continuous optimization by regularly reviewing and refining cost-saving strategies based on evolving business needs, technological advancements, and cloud provider offerings (Continuous Optimization). **6.2.2.14.** Provide ongoing training to educate users on cost-effective cloud resource management practices, empowering them to make informed decisions that align with cost-saving objectives. **6.2.2.15.** Engage in regular negotiations with cloud service providers to explore cost-saving opportunities, such as volume discounts, reserved capacity commitments, or customized pricing models.

6.3. SECURITY BASELINE:

Security configuration requirements for all Cloud Systems.	
Justification / Description	The effectiveness of Cloud services depends on how it is implemented within an organization. Below are the controls that must be complied with when configuring cloud services.
Standard Requirements	The following requirements must be complied with: **6.3.1.** <u>**Data protection:**</u> **6.3.1.1.** All cloud-based Transnet Data, both structured and unstructured, will be managed in line with data classification policy and standard. **6.3.1.2.** Microsoft OneDrive is the authorised cloud platform for storing and sharing company information. Any other public cloud-based services example Google drive, iCloud, and/or Dropbox must not be used for sharing and/or storing company information. Cloud based services hosted by third parties must be approved prior unless explicitly approved for business use. **6.3.1.3.** If at any point the flow of data will contain personally identifiable information (PII), credit card numbers, data covered under POPI Act, confidential corporate data or any other sensitive or regulated data, the data must be encrypted two ways (to and from the cloud provider) and when in storage (refer to section 6.4.3 "Tagging"). **6.3.1.4.** Any usage of cloud services must adhere to all applicable laws, Policies, Standards, and regulations governing Transnet. **6.3.2.** <u>**AZURE: Role Based Access Control (RBAC):**</u> All deployments must have RBAC provisioned through the relevant portal / mechanisms to ensure roles are provisioned at the fabric layer and not only on the Virtual Machines (VMs). The principle of least privilege access applies. Role changes must be tracked, and role assignment alerts must be enabled.

Refer to the below list of available built-in RBAC roles available within Microsoft Azure:

Built-in role	Description
Owner	Let's you manage everything, including access to resources.
Contributor	Let's you manage everything except access to resources.
Reader	Let's you view everything, but not make any changes.
AcrImageSigner	acr image signer
AcrQuarantineReader	acr quarantine data reader
AcrQuarantineWriter	acr quarantine data writer
API Management Service Contributor	Can manage service and the APIs
API Management Service Operator Role	Can manage service but not the APIs
API Management Service Reader Role	Read-only access to service and APIs
Application Insights Component Contributor	Can manage Application Insights components
Application Insights Snapshot Debugger	Gives user permission to use Application Insights Snapshot Debugger features
Automation Job Operator	Create and Manage Jobs using Automation Runbooks.
Automation Operator	Automation Operators can start, stop, suspend, and resume jobs
Automation Runbook Operator	Read Runbook properties - to be able to create Jobs of the runbook.
Azure Stack Registration Owner	Let's you manage Azure Stack registrations.
Backup Contributor	Let's you manage backup service, but can't create vaults and give access to others
Backup Operator	Let's you manage backup services, except removal of backup, vault creation and giving access to others
Backup Reader	Can view backup services, but can't make changes
Billing Reader	Allows read access to billing data
BizTalk Contributor	Let's you manage BizTalk services, but not access to them.
CDN Endpoint Contributor	Can manage CDN endpoints but can't grant access to other users.
CDN Endpoint Reader	Can view CDN endpoints but can't make changes.

CDN Profile Contributor	Can manage CDN profiles and their endpoints but can't grant access to other users.
CDN Profile Reader	Can view CDN profiles and their endpoints but can't make changes.
Classic Network Contributor	Let's you manage classic networks, but not access to them.
Classic Storage Account Contributor	Let's you manage classic storage accounts, but not access to them.
Classic Storage Account Key Operator Service Role	Classic Storage Account Key Operators are allowed to list and regenerate keys on Classic Storage Accounts
Classic Virtual Machine Contributor	Let's you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
ClearDB MySQL DB Contributor	Let's you manage ClearDB MySQL databases, but not access to them.
Cosmos DB Account Reader Role	Can read Azure Cosmos DB account data. See DocumentDB Account Contributor for managing Azure Cosmos DB accounts.
Data Factory Contributor	Create and manage data factories, as well as child resources within them.
Data Lake Analytics Developer	Let's you submit, monitor, and manage your own jobs but not create or delete Data Lake Analytics accounts.
Data Purger	Can purge analytics data
DevTest Labs User	Let's you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.
DNS Zone Contributor	Let's you manage DNS zones and record sets in Azure DNS but does not let you control who has access to them.
DocumentDB Account Contributor	Can manage Azure Cosmos DB accounts. Azure Cosmos DB is formerly known as DocumentDB.
Intelligent Systems Account Contributor	Let's you manage Intelligent Systems accounts, but not access to them.
Key Vault Contributor	Let's you manage key vaults, but not access to them.
Lab Creator	Let's you create, manage, delete your managed labs under your Azure Lab Accounts.

Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; reading storage account keys to be able to configure collection of logs from Azure Storage; creating and configuring Automation accounts; adding solutions; and configuring Azure diagnostics on all Azure resources.
Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure diagnostics on all Azure resources.
Logic App Contributor	Let's you manage logic app, but not access to them.
Logic App Operator	Let's you read, enable, and disable logic app.
Managed Identity Contributor	Create, Read, Update, and Delete User Assigned Identity
Managed Identity Operator	Read and Assign User Assigned Identity
Monitoring Contributor	Can read all monitoring data and edit monitoring settings. See also Get started with roles, permissions, and security with Azure Monitor.
Monitoring Reader	Can read all monitoring data (metrics, logs, etc.). See also Get started with roles, permissions, and security with Azure Monitor.
Network Contributor	Let's you manage networks, but not access to them.
New Relic APM Account Contributor	Let's you manage New Relic Application Performance Management accounts and applications, but not access to them.
Reader and Data Access	Let's you view everything but will not let you delete or create a storage account or contained resource. It will also allow read/write access to all data contained in a storage account via access to storage account keys.
Redis Cache Contributor	Let's you manage Redis caches, but not access to them.
Resource Policy Contributor (Preview)	(Preview) Backfilled users from EA, with rights to create/modify resource policy, create support ticket and read resources/hierarchy.
Scheduler Job Collections Contributor	Let's you manage Scheduler job collections, but not access to them.

Search Service Contributor	Let's you manage Search services, but not access to them.
Security Admin	In Security Center only: Can view security policies, view security states, edit security policies, view alerts and recommendations, dismiss alerts and recommendations
Security Manager (Legacy)	This is a legacy role. Please use Security Administrator instead
Security Reader	In Security Center only: Can view recommendations and alerts, view security policies, view security states, but cannot make changes
Site Recovery Contributor	Let's you manage Site Recovery service except vault creation and role assignment
Site Recovery Operator	Let's you failover and failback but not perform other Site Recovery management operations
Site Recovery Reader	Let's you view Site Recovery status but not perform other management operations
SQL DB Contributor	Let's you manage SQL databases, but not access to them. Also, you can't manage their security-related policies or their parent SQL servers.
SQL Security Manager	Let's you manage the security-related policies of SQL servers and databases, but not access to them.
SQL Server Contributor	Let's you manage SQL servers and databases, but not access to them, and not their security -related policies.
Storage Account Contributor	Let's you manage storage accounts, but not access to them.
Storage Account Key Operator Service Role	Storage Account Key Operators are allowed to list and regenerate keys on Storage Accounts
Storage Blob Data Contributor (Preview)	Allows for read, write, and delete access to Azure Storage blob containers and data
Storage Blob Data Reader (Preview)	Allows for read access to Azure Storage blob containers and data
Storage Queue Data Contributor (Preview)	Allows for read, write, and delete access to Azure Storage queues and queue messages
Storage Queue Data Reader (Preview)	Allows for read access to Azure Storage queues and queue messages
Support Request Contributor	Let's you create and manage Support requests

Traffic Manager Contributor	Let's you manage Traffic Manager profiles but does not let you control who has access to them.
User Access Administrator	Let's you manage user access to Azure resources.
Virtual Machine Administrator Login	- Users with this role can login to a virtual machine with Windows administrator or Linux root user privileges.
Virtual Machine Contributor	Let's you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
Virtual Machine User Login	Users with this role can login to a virtual machine as a regular user.
Web Plan Contributor	Let's you manage the web plans for websites, but not access to them.
Website Contributor	Let's you manage websites (not web plans), but not access to them.

6.3.3. Network Security Groups (NSG) and Default Configurations:

6.3.3.1. Configuration of the NSGs comprises of defaults loaded by the Azure Fabric for basic protection and custom rules that are configured once the NSG has been deployed.

6.3.3.2. NSG security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port and protocol) to allow or deny the traffic. A Flow record is created for existing connections, communication is allowed or denied based on the connection state of the flow records, this allows NSG to be stateful. If you specify an outbound security rule to any address over port 80, for example, it is not necessary to specify an inbound security rule for the response to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally. The opposite is also true. If inbound traffic is allowed over a port, it is not necessary to specify an outbound security rule to respond to traffic over the port. An existing connection must not be interrupted when you remove a security rule that enabled the flow. Traffic flows are interrupted when connections are stopped, and no traffic is flowing on either direction for at least a few minutes.

A breakdown of the fields and associated options are noted below:

Priority:	*Rules are processed in priority order, the lower the number, the higher the priority. It is recommended to leave gaps between rules - 100, 200, 300, etc. - so that it's easier to add new rules without having to edit existing rules*

Name:	*Name of the rule to distinguish it from others. This is a unique identifier for each rule*
Port:	*This specifies on which ports traffic will be allowed or denied by this rule.* *Provide a single port such as 80; a port range such as 1024-65535 or a comma-separated list of single ports and/or port ranges such as 80, 1024-65535. Provide and asterisk (*) to allow traffic on any port.*
Protocol:	*This is the traffic protocol being allowed/denied through the NSG. I.e., All / TCP / UDP*
Source:	*The source filter can be Any, a specific address / address range or a default tag. It specifies the incoming traffic source IP range that will be allowed or denied by this rule.*
Destination:	*The destination filter can be Any, an IP address/range, or a default tag. It specifies the outgoing traffic for a specific destination IP address range that will be allowed or denied by this rule.*
Action:	*This is noting whether you are allowing or denying traffic through based on the settings configured*

6.3.4. Augmented Security Rules

6.3.4.1. An additional form of security rules is available using Augmented security rules to make rule management easier for predetermined sources and destinations. This list is controlled by Microsoft and cannot be edited to suit a customer's unique requirements due to the functionality being part of the Azure Fabric.

6.3.4.2. *"Augmented rules simplify security definition for virtual networks, allowing you to define larger and complex network security policies, with fewer rules. You can combine multiple ports, multiple explicit IP addresses, Service tags, and Application security groups into a single, easily understood security rule. Use augmented rules in the source, destination, and port fields of a rule. When creating a rule, you can specify multiple explicit IP addresses, CIDR (Classless Inter-Domain Routing) ranges, and ports. To simplify maintenance of your security rule definition, combine augmented security rules with service tags or application security groups."*

Below is a selection of the Service Tags available when configuring NSG rules:

Virtual Network	*This tag includes the virtual network address space (all CIDR ranges defined for the virtual network), all connected on-premises address spaces, and peered virtual networks or virtual network connected to a virtual network gateway.*

	Azure Load Balancer	*This tag denotes Azure's infrastructure load balancer. The tag translates to an Azure datacenter IP (Internet Protocol) address where Azure's health probes originate. If you are not using the Azure load balancer, you can override this rule.*
	Internet	*This tag denotes the IP address space that is outside the virtual network and reachable by the public Internet. The address range includes the Azure owned public IP address space.*
	Azure Traffic Manager	*This tag denotes the IP address space for the Azure Traffic Manager probe IPs. More information on Traffic Manager probe IPs can be found in the Azure Traffic Manager FAQ.*
	Storage	*This tag denotes the IP address space for the Azure Storage service. If you specify Storage for the value, traffic is allowed or denied to storage. If you only want to allow access to storage in a specific region, you can specify the region. For example, if you want to allow access only to Azure Storage in the East US region, you could specify Storage.EastUS as a service tag. The tag represents the service, but not specific instances of the service. For example, the tag represents the Azure Storage service, but not a specific Azure Storage account. All address prefixes represented by this tag are also represented by the Internet tag.*
	SQL	*This tag denotes the address prefixes of the Azure SQL Database and Azure SQL Data Warehouse services. If you specify SQL for the value, traffic is allowed or denied to SQL. If you only want to allow access to SQL in a specific region, you can specify the region. For example, if you want to allow access only to Azure SQL Database in the East US region, you could specify SQL. EastUS as a service tag. The tag represents the service, but not specific instances of the service. For example, the tag represents the Azure SQL Database service, but not a specific SQL database or server. All address prefixes represented by this tag are also represented by the Internet tag.*
	Azure Cosmos DB	*This tag denotes the address prefixes of the Azure Cosmos Database service. If you specify AzureCosmosDB for the value, traffic is allowed or denied to AzureCosmosDB. If you only want to allow access to AzureCosmosDB in a specific region, you can specify the region in the following format AzureCosmosDB.[region name].*

Azure Key Vault	*This tag denotes the address prefixes of the Azure Key Vault service. If you specify AzureKeyVault for the value, traffic is allowed or denied to AzureKeyVault. If you only want to allow access to AzureKeyVault in a specific region, you can specify the region in the following format AzureKeyVault.[region name].*

6.3.5. Default NSG Rules on Deployment

When a NSG is deployed there is a predetermined set of default rules applied. The Change Advisory Board (CAB) process must be followed for the approval of creating custom security groups.

Below is a breakdown of the default rules applied:

6.3.5.1. Inbound Default rules

Allow VNet In Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	Virtual Network	0-65535	Virtual Network	0-65535	All	Allow

Allow Azure Load Balancer In Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	Azure Load Balancer	0-65535	0.0.0.0/0	0-65535	All	Allow

Deny All Inbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

6.3.5.2. Outbound Default rules

Allow Vnet Out Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	Virtual Network	0-65535	Virtual Network	0-65535	All	Allow

Allow Internet Out Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	All	Allow

Deny All Out Bound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

Refer to the Transnet Web Server Standard and the Network security Standard. (Transnet Standards)

6.4. RESOURCE CONSISTENCY

Resource consistency on all cloud Systems	
Justification / Description	The effectiveness of a resource consistency depends on how it is implemented within an organization. Below are the controls that must be compiled with when initiating cloud services: Virtual systems must be clearly identified and documented to enable the effective management of cloud infrastructure.
Standard Requirements	The following requirements must be complied with: **6.4.1. <u>Maintain a CMDB of all workloads deployed:</u>** **6.4.1.1.** All deployments of cloud-based solutions to be documented on the Transnet CMDB. **6.4.1.2.** Changes to cloud-based deployments can be maintained through Infrastructure as code (IaC) (e.g., Terraform declarative configuration files, deployed via pipeline and source controlled) **6.4.2. <u>Data Classifications and Restrictions:</u>** All data moving to and through Transnet's usage of cloud services are subject to and must adhere to organizationally defined data classification levels. This classification includes all the levels as defined in the Classification Policy (Data for public consumption and data for private consumption). The Group CIO may after consultation with Chief Corporate and Regulatory Officer determine how Transnet data is to be managed whilst on the cloud platform. **6.4.3. <u>Tagging Definitions and Standards:</u>** **6.4.3.1. Database Server:** 1) Environment - AZ (AZURE) 2) OS version - W (windows) / L (Linux) 3) OD - TCC 4) Abbreviated Application (workload)- PRIM (Primavera) 5) Database - DB 6) Number - 101 following 102 following 103 7) Stored Data Classification level - Public/Confidential/Secret 8) Business Unit - HR/Marketing/ICT/Finance 9) Development / Production - Dev / Prod Example: AZWTCCPRIMDB_HR_Prod101

6.4.3.2. Resource Group:

1)	Group	- RG
2)	Operating Division	- TCC
3)	Abbreviated Application (Workload)	- PRIM (Primavera)

Example: RG–TCC–PRIM

6.4.3.3. Server:

1)	Environment	- AZ (AZURE)
10)	OS version	- W (windows) / L (Linux)
2)	Operating Division	- TCC
3)	Abbreviated Application (Workload)	- PRIM (Primavera)
4)	Server	- SRV
5)	Number	- 101 following 102 following 103
6)	Stored Data Classification level	- Public/Confidential/Secret
7)	Business Unit	- HR/Marketing/ICT/Finance
8)	Development / Production	- Dev / Prod

Example: AZWTCCPRIMSRV_FIN_Dev101

6.5. CLOUD DEPLOYMENTS

Cloud Deployments	
Justification / Description	The effectiveness of Cloud services depends on how it is implemented within an organization. Below are the controls that must be complied with when configuring cloud services.
Standard Requirements	The following requirements must be complied with: **6.5.1. General Requirements:** **6.5.1.1.** Transnet must have a single tenant with operating divisions configured as departments under the single subscription. Each OD (Operating Division) will then register accounts and subscriptions under the relevant OD. **6.5.1.2.** Any cloud workloads must go to Change Advisory Board (CAB) for formal approval (including DEV, QA, and Production systems). **6.5.1.3.** For all cloud deployments (e.g., SaaS, PaaS, IaaS), at minimum obtain an annual SOC (Security Operations Center) Type 2 report and/or ISO 27001 certification from the contracted cloud service provider (CSP) / operating service provider (OSP) and ensure they meet the minimum requirements. **6.5.1.4.** Use of cloud computing services for work purposes must be formally authorized by the Operating division head of ICT or DOA (Delegation of Authority). The OD head of ICT or DOA must certify that security, privacy, and all other IT management requirements will be adequately addressed by the cloud computing vendor. **6.5.1.5.** Before entering into any new contract or agreement with a cloud vendor, a thorough due diligence must be conducted to ensure that the vendor's services align with the security, privacy, compliance, and operational requirements of Transnet. This aims to minimize risks, safeguard sensitive information, and ensure the continuity of our operations while leveraging the benefits of cloud-based services. This due diligence process includes at a minimum the following steps: 1) **Security Assessment:** Evaluating the vendor's security measures, including data encryption practices, access controls, network security protocols, and incident response procedures. 2) **Privacy Compliance:** Verifying that the vendor complies with applicable privacy regulations, such as GDPR, CCPA, HIPAA, or any other relevant standards, and assessing their data handling and privacy protection mechanisms. 3) **Compliance Certification:** Confirming that the vendor adheres to industry-specific compliance standards, such as SOC 2, ISO 27001, PCI DSS, or others relevant to our business operations.

Cloud Deployments

4) **Data Residency and Sovereignty:** Ensuring that the vendor's data storage and processing locations comply with our legal and regulatory requirements regarding data residency and sovereignty.
5) **Service Level Agreements (SLAs):** Reviewing SLAs to understand the vendor's commitments regarding uptime, performance, support, and resolution times for issues or disruptions.
6) **Vendor reputation and Reliability:** Assessing the vendor's reputation, reliability, financial stability, and track record of delivering high-quality services to other clients.
7) **Exit Strategy and Data Portability:** Establishing procedures and mechanisms for data migration, termination of services, and ensuring data portability in the event of contract termination or vendor changes.
8) **Risk Management:** Identifying and mitigating potential risks associated with the vendor's services, including vendor lock-in, service disruptions, data breaches, and legal liabilities.

6.5.1.6. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the OD Head of ICT or DOA.

6.5.1.7. The use of such services must comply with Transnet Acceptable Use and Transnet Information Security Policy.

6.5.1.8. The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Transnet.

6.5.1.9. The OD Head of ICT or DOA decides what data may or may not be stored in the Cloud.

6.5.1.10. Below is a set of standards that must be applied to all cloud-based deployments. Due to the list of available services or workloads this document does not provide granular detail for configuration standards and therefore require that the cloud administrator ensures that deployments are done looking at best-practise while ensuring all standards noted in this document are adhered to.

6.5.2. **Generic standards across subscriptions:**

6.5.2.1. All deployments to have anti-malware installed.

6.5.2.2. All deployments to be placed in the South African region.

6.5.2.3. All disks and databases deployed to have encryption.

6.5.2.4. All workloads, components, resource groups to be tagged for their purpose – Tagging definition and standard to be defined.

6.5.2.5. All passwords created during deployment are to be either 42 characters or use certificate authentication. The password may be securely stored in a PAM (Privileged Access Management) or password manager.

6.5.2.6. All IP addresses to be dynamic unless there is a business and technical need for static IP addressing.

6.5.3. **Production deployments:**

6.5.3.1. All production deployments to be part of high availability sets.

6.5.3.2. All production deployments to have OMS (Operations Management Suite) monitoring.

6.5.3.3. All production deployments to have backup and disaster recovery enabled.

6.5.3.4. All production deployments to have change tracking enabled.

6.5.3.5. All production deployments to have alerts enabled and configured.

6.5.3.6. Use of Premium disks is limited to deployments that require high Input/Output rates.

6.5.3.7. All production deployments to have disks managed as part of the managed disks feature.

6.5.3.8. All production deployments to have Just in Time VM (Virtual Machine) access enabled.

6.5.3.9. The use of external IP addresses is limited to workloads that need direct internet facing connections. By default, all workloads will have this disabled as all traffic will route through load balancers. However, this is a workload and design dependant.

6.5.3.10. Regular reviews and monitoring must be performed for external facing IPs. Alerts must be configured for the creation of public IPs.

6.5.3.11. All VMs are to have disk encryption enabled.

6.5.4. **Development and Testing deployments**

6.5.4.1. Dev/Test deployments not to have high availability outside of the High availability PoC (Proof of Concept).

6.5.4.2. Masking requirements for the usage of production data in development/test environments in cloud computing:

1) **Data Anonymization:** Ensure that personally identifiable information (PII), such as names, addresses, social security numbers, and other sensitive data, is anonymized or replaced with

synthetic data that retains the format and structure but does not contain real information.

2) **Tokenization:** Implement tokenization techniques to replace sensitive data with randomly generated tokens while preserving referential integrity and ensuring that the tokens cannot be reverse engineered to retrieve the original data.
3) **Pseudonymization:** Use pseudonymization methods to replace identifiable information with pseudonyms or aliases, which are reversible only with access to a separate mapping table stored securely and accessible only to authorized personnel.
4) **Subset Selection:** Limit the amount of production data used in development/test environments by selecting a subset of records or data fields that are necessary for testing purposes while excluding unnecessary or sensitive information.
5) **Data Masking Techniques:** Employ data masking techniques such as substitution, shuffling, encryption, or format-preserving encryption to obfuscate sensitive data while maintaining its usability for testing and development activities.
6) **Dynamic Data Masking:** Implement dynamic data masking mechanisms that dynamically conceal sensitive data in real-time based on user roles and privileges, ensuring that unauthorized users do not have access to sensitive information even within the development/test environment.
7) **Data De-identification:** De-identify sensitive data by removing direct identifiers and suppressing quasi-identifiers to minimize the risk of re-identification while maintaining the utility of the data for testing and development purposes.
8) **Data Lifecycle Management:** Establish policies and procedures for the lifecycle management of masked production data in development/test environments, including data generation, masking, storage, usage, and disposal, to ensure compliance with regulatory requirements and minimize data exposure.
9) **Monitoring and Auditing:** Implement monitoring and auditing mechanisms to track and log access to masked production data in development/test environments, detect unauthorized access or usage, and maintain accountability for data handling activities.

6.5.4.3. OMS (Azure Operations Management Suite) monitoring is required on Dev/Test deployments as it is best for pre-production environments to be mirrors of production. Not having OMS monitoring during the Dev and Testing phase may introduce risks or result in outages, when released to production.

6.5.4.4. Disaster recovery is not required on Dev/Test workloads.

6.5.4.5. Cost management visibility alerts must be configured for Dev/Test deployments.

6.5.4.6. Premium storage is not to be used for dev test deployments.

6.5.4.7. Disks to be managed as part of the managed disks feature.

Cloud Deployments	
	6.5.4.8. Just in time VM access can be enabled depending on technical requirement. **6.5.4.9.** No Dev Test deployment is to use public IP addresses unless there is a technical and business requirement that is approved. **6.5.4.10.** Disk encryption is not mandatory and is at the discretion of the business owner. **6.5.4.11.** All Dev test deployments to have auto-shutdown enabled.

7. EXCEPTIONS

Conformance with this standard is mandatory and whilst the necessary care must be taken to ensure that the requirements within this standard are as practical as possible, situations may arise where compliance to specific requirements may not be feasible/possible. For all cases where compliance to a specific requirement is not possible, an exemption or exception must be formally submitted in line with the deviation process. Such deviation requests must be submitted to the GM: Technology Innovation & Digital Transformation for preliminary investigations and considerations. Only the Information Security, Governance, Risk and Compliance Committee has the authority to formally approve deviations from this standard.

8. REFERENCES

The Standard must be read in conjunction with the following related internal and external requirements:

8.1. INTERNAL DOCUMENTS:

- Information Security Policy.
- Information Classification Policy & Standard.
- Cryptography Standard.
- Enterprise Risk Management Strategy and Framework.
- ICT Continuity Standard.
- ICT Physical and environmental Security Standard.
- ICT Vulnerability & Patch Management Standard.
- Network Security Standard.
- Web Server Standard.
- Incident Management Standard.
- User and Device Management Standard.

8.2. EXTERNAL DOCUMENTS:

- Azure Well-Architected Framework.
- The Protection of Personal Information Act, 2013 (Act No 4 of 2013).
- The King IV Report on Corporate Governance for South Africa.
- Electronic Communications Act 36 of 2005.
- Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002.

9. VIOLATIONS OF THE STANDARD

Each employee is responsible for complying with the Cloud Standard requirements. Violation of any provision of this Standard will result in one or more of the following:

- Total or partial limitation of an employee's or third party's access to some or all of Transnet's systems.
- Initiation of legal action by Transnet including, but not limited to, criminal or civil prosecution under the applicable law.
- Transnet requiring the violator to provide restitution for any improper use of service.
- Disciplinary sanctions against employees.
- Invocation or legal remedies such as those included in contractual agreements and Service Level Agreements including cancellation of contracts with third parties.

Port	Terminal	Equipment	Available
CPT	CTCT	Straddle Carriers	12
CPT	CTCT	RTG cranes	32
CPT	CTCT	Haulers	75
CPT	CTCT	Empty Container Handler	7
CPT	CTCT	Reach Stackers	2
CPT	CTCT	Mobile Bowser	2
CPT	CTCT	Fuel Tanks	2
CPT	CTCT	Dispenser Pump	1
CPT	CTMPT	Straddle Carriers	8
CPT	CTMPT	Mobile Harbour Cranes	3
CPT	CTMPT	Haulers	16
CPT	CTMPT	Reach Stackers	3
CPT	CTMPT	13 - 45Forklifts	5
CPT	CTMPT	3T Heli Forklifts	3
CPT	CTMPT	5T TCM - Forklits	2
CPT	CTMPT	Mobile Bowser	1
DBN	DCT Pier 1	RTG cranes	25
DBN	DCT Pier 1	Haulers	47
DBN	DCT Pier 1	Reach Stackers	4
DBN	DCT Pier 1	Mobile Bowser	2
DBN	DCT Pier 1	Fuel Tanks	2
DBN	DCT Pier 1	Dispenser Pump	2
DBN	DCT Pier 2	Straddle Carriers	108
DBN	DCT Pier 2	Haulers	75
DBN	DCT Pier 2	Reach Stackers	3
DBN	DCT Pier 2	Empty Container Handler	10
DBN	DCT Pier 2	Mobile Bowser	2
DBN	DCT Pier 2	Fuel Tanks	4
DBN	DCT Pier 2	Dispenser Pump	8
DBN	Maydorn Wharf	Haulers	8
DBN	Maydorn Wharf	Tractors	15
DBN	Maydorn Wharf	Reach Stackers	2
DBN	Maydorn Wharf	Forklifts	3
DBN	Maydorn Wharf	Mobile Bowser	1
DBN	Maydorn Wharf	Fuel Tanks	1
DBN	Maydorn Wharf	Dispenser Pump	1
DBN	Point	Mobile Harbour Cranes	4
DBN	Point	Haulers	37
DBN	Point	Reach Stackers	15
DBN	Point	Forklifts	3
DBN	Point	Mobile Bowser	1
DBN	Point	Fuel Tanks	1
DBN	Point	Dispenser Pump	1
EL	ELMPT	Grain Elevators	2
EL	ELMPT	Straddle Carriers	4
EL	ELMPT	Mobile Bowser	1
EL	ELMPT	Fuel Tanks	2
EL	ELMPT	Dispenser Pump	2
NGQ	NCT	RTG cranes	37
NGQ	NCT	Reach Stackers	4
NGQ	NCT	Empty Container Handler	6
NGQ	NCT	Haulers	98
NGQ	NCT	Mobile Bowser	2
NGQ	NCT	Fuel Tanks	4
NGQ	NCT	Dispenser Pump	6
PE	PE BULK	Stackers	2

PE	PE BULK	Reclaimers	3
PE	PE BULK	30 Ton Forklifts	1
PE	PECT	Straddle Carriers	21
PE	PECT	Mobile Harbour Cranes	1
PE	PECT	Reach Stackers	2
PE	PECT	Empty Container Handler	2
PE	PECT	Mobile Bowser	1
PE	PECT	Fuel Tanks	2
PE	PECT	Dispenser Pump	3
PE	PEMT	H & T	2
RCB	RCB DBT	Stackers	2
RCB	RCB DBT	Mobile Harbour Cranes	3
RCB	RCB DBT	Hoppers	2
RCB	RCB MPT	Reach Stackers	3
RCB	RCB MPT	Terberg Haulers	69
RCB	RCB MPT	Mobile Harbour Cranes	1
RCB	RCB MPT	Ferrari Haulers	4
RCB	RCB MPT	Mafi Haulers	2
RCB	RCB MPT	42T Forklifts	3
RCB	RCB MPT	32T Forklifts	6
RCB	RCB MPT	18T Forklifts	10
RCB	RCB MPT	8T Forklifts	11
RCB	RCB MPT	Water Tankers	3
RCB	RCB MPT	Excavators	11
RCB	RCB MPT	Bobcats	6
RCB	RCB MPT	Bobcat Sweepers	2
RCB	RCB MPT	Mobile Bowser	2
RCB	RCB MPT	Fuel Tanks	3
RCB	RCB MPT	Dispenser Pump	6
SAL	SLD MPT	Forklifts	12
SAL	SLD MPT	Terberg Haulers	14
SAL	SLD MPT	Mobile Shiploaders	2
SAL	SLD MPT	Mobile Bowser	1
SAL	SLD MPT	Fuel Tanks	2
SAL	SLD MPT	Dispenser Pump	2
NORTHERN CAPE	LOHATLA	Motor Vechicles	3
NORTHERN CAPE	LOHATLA	Heavy duty Machines / FEL	4
NORTHERN CAPE	LOHATLA	Excavators	1
NORTHERN CAPE	LOHATLA	Generator (Back up)	1
NORTHERN CAPE	LOHATLA	Locomotives	3
NORTHERN CAPE	LOHATLA	Mobile Bowser	1
NORTHERN CAPE	LOHATLA	Fuel Tanks	2
NORTHERN CAPE	LOHATLA	Dispenser Pump	2
NORTHERN WEST	PENDORING	Heavy duty Machines / FEL	3
NORTHERN WEST	PENDORING	Bobcat	3
NORTHERN WEST	PENDORING	Water Tankers	3
NORTHERN WEST	PENDORING	Mobile Bowser	1
NORTHERN WEST	PENDORING	Fuel Tanks	1
NORTHERN WEST	PENDORING	Dispenser Pump	1
MPUMALANGA	KENDAL	Heavy duty Machines / FEL	3
MPUMALANGA	KENDAL	Bobcat	3
MPUMALANGA	KENDAL	Water Tankers	3
MPUMALANGA	KENDAL	Mobile Bowser	1
MPUMALANGA	KENDAL	Fuel Tanks	2
MPUMALANGA	KENDAL	Dispenser Pump	2