




TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 1 of 68


SCADA System Architecture Failure and Recovery Mode Analysis

E354086-00000-271-078-0013

REV. 03

DOCUMENT APPROVAL PROCESS

NAME		POSITION/MEETING NO.	SIGNATURE	DATE
Originator:	Hugo Rust	Lead SCADA Engineer		07-09-2020
Approver:	Klasie Badenhorst	Project Manager		07-09-2020
Original date: 10-07-2018				
Effective date: 07-09-2020				

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 2 of 68

DOCUMENT CHANGE HISTORY:

Date	Previous Rev No.	New Rev No.	Details of Revision
02-02-2022	02	03	As Built




TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 3 of 68

TABLE OF CONTENTS


1	INTRODUCTION	10
1.1	Purpose	10
1.2	Scope	10
1.2.1	Requirements Included.....	10
1.2.2	Requirements Excluded	10
1.3	Terms and Definitions	10
1.3.1	Abbreviations.....	10
1.3.2	Definitions	11
2	APPLICABLE DOCUMENTS	13
2.1	TPL Applicable Specifications and Standards.....	13
2.2	Other Applicable Specifications and Standards	14
2.3	Reference Documentation	14
3	TPL SYSTEM.....	15
3.1	System Availability	15
3.2	System Architectures	15
3.3	Physical Architecture	17
3.4	System Architecture	17
3.5	Coalbrook (CBK) Intake/Delivery Station Architecture	20
3.6	Fynnlads (FYN) Intake Station Architecture	21
3.7	Pump / Booster Station Architecture	22
4	SYSTEM AVAILABILITY	23
4.1	Availability Considerations	23
4.1.1	Redundant LAN Network	23
4.2	Software Redundancy	23

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 4 of 68


4.3	Availability Formulas	24
4.4	Component Reliability and Availability	24
4.5	Production System Availability	26
4.5.1	Primary Production System Availability	26
4.5.2	Primary Station System Availability	26
4.6	Total Production System Availability	26
5	FAILURE PROTECTION.....	29
5.1	Overview.....	29
5.2	OASyS Services	30
5.2.1	OASyS Service Failure	30
5.2.2	OASyS Station Failure.....	30
5.3	OASyS DistribuSyS and Modes.....	31
5.3.1	Overview	31
5.4	Failure Modes.....	32
5.4.1	Redundant Station SCADA Service Failure.....	32
5.4.2	Non-Redundant Station SCADA Service Failure.....	32
5.4.3	Non-Redundant Station Workstation Failure.....	33
5.5	Limited or Complete Loss of Communications	34
5.5.1	Loss of Communication with Field Equipment.....	34
5.5.2	Loss of Communication between Station and MCC	34
6	FAILURE AND RECOVERY	35
6.1	Network Interface Card (NIC) Connection Failure	35
6.1.1	Single NIC Connection Failure	35
6.1.2	Dual NIC Connection Failure	35
6.2	Local Area Network (LAN) Switch Failure.....	37

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 5 of 68


6.2.1	Single Switch Failure	37
6.2.2	Dual Switch Failure	37
6.3	Storage Area Network (SAN) Failure	39
6.3.1	SAN Component Failure.....	39
6.3.2	SAN Failure.....	39
6.4	Virtual Guest Server Failure	41
6.4.1	Failed Component and Description of Failure	41
6.4.2	Impact on Operations / System and Severity	41
6.4.3	Typical Cause of Failure.....	41
6.4.4	Means of detection and controls.....	41
6.4.5	Rectification and Impact of Rectification	41
6.4.6	Preventative Maintenance.....	42
6.5	Leak Detection System (LDS) Service Failure	43
6.5.1	Failed Component and Description of Failure	43
6.5.2	Impact on Operations / System and Severity	43
6.5.3	Typical Cause of Failure.....	43
6.5.4	Means of Detection and Controls.....	43
6.5.5	Rectification and Impact of Rectification	43
6.5.6	Preventative Maintenance.....	43
6.6	OASyS Services Failure.....	44
6.6.1	Failed Component and Description of Failure	44
6.6.2	Impact on Operations / System and Severity	44
6.6.3	Typical Cause of Failure.....	44
6.6.4	Means of Detection and Controls.....	44
6.6.5	Rectification and Impact of Rectification	44

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 6 of 68


6.6.6	Preventative Maintenance.....	45
6.7	OASyS Software Application Failure	46
6.7.1	Failed Component and Description of Failure	46
6.7.2	Impact on Operations / System and Severity	46
6.7.3	Typical Cause of Failure.....	46
6.7.4	Means of Detection and Controls.....	46
6.7.5	Rectification and Impact of Rectification	46
6.7.6	Preventative Maintenance.....	47
6.8	Domain Controller (DC) Failure	48
6.8.1	Failed Component and Description of Failure	48
6.8.2	Impact on Operations/System and Severity	48
6.8.3	Typical Cause of Failure.....	48
6.8.4	Means of Detection and Controls.....	48
6.8.5	Rectification and Impact of Rectification	48
6.8.6	Preventative Maintenance.....	48
6.9	Time Server Failure.....	49
6.9.1	Failed Component and Description of Failure	49
6.9.2	Impact on Operations / System and Severity	49
6.9.3	Typical Cause of Failure.....	49
6.9.4	Means of Detection and Controls.....	49
6.9.5	Rectification and Impact of Rectification	49
6.9.6	Preventative Maintenance.....	49
6.10	Network Security Appliance (Firewall Failure)	50
6.10.1	Failed Component and Description of Failure	50
6.10.2	Impact on Operations / System and Severity	50

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 7 of 68

6.10.3	Typical Cause of Failure.....	50
6.10.4	Means of Detection and Controls.....	50
6.10.5	Rectification and Impact of Rectification	51
6.10.6	Preventative Maintenance.....	51
6.11	Decision Support System (DSS) Failure	52
6.11.1	Failed Component and Description of Failure	52
6.11.2	Impact on Operations / System and Severity	52
6.11.3	Typical Cause of Failure.....	52
6.11.4	Means of detection and controls.....	52
6.11.5	Rectification and Impact of Rectification	52
6.11.6	Preventative Maintenance.....	52
6.12	Workstation Failure.....	53
6.12.1	Failed component and description of the failure	53
6.12.2	Impact on Operations / System and Severity	53
6.12.3	Typical Cause of Failure.....	53
6.12.4	Means of Detection and Controls.....	53
6.12.5	Rectification and Impact of Rectification	53
6.12.6	Preventative Maintenance.....	53
6.13	Historical Playback Data Capture Failure.....	54
6.13.1	Failed Component and Description of Failure	54
6.13.2	Impact on Operations / System and Severity	54
6.13.3	Typical Cause of Failure.....	54
6.13.4	Means of Detection and Controls.....	54
6.13.5	Rectification and Impact of Rectification	54
6.13.6	Preventative Maintenance.....	54

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 8 of 68

6.14	SCADA System Communication to PLC Failure	55
6.14.1	Failed Component and Description of Failure	55
6.14.2	Impact on Operations / System and Severity	55
6.14.3	Typical Cause of Failure.....	55
6.14.4	Means of Detection and Controls.....	55
6.14.5	Rectification and Impact of Rectification	55
6.14.6	Preventative Maintenance.....	55
6.15	SAP Interface Failure (Via DSS)	56
6.15.1	Failed Component and Description of Failure	56
6.15.2	Impact on Operations / System and Severity	56
6.15.3	Typical Cause of Failure.....	56
6.15.4	Means of Detection and Controls.....	56
6.15.5	Rectification and Impact of Rectification	56
6.15.6	Preventative Maintenance.....	56
6.16	Metering	57
6.16.1	PRV FC Failure to OASyS (Modbus Interface) – Total Loss Interface (1,4).....	57
6.16.2	STM FC Failure to OASyS (Modbus Interface) – Total Loss of Interface (1,4)	58
6.16.3	Host Failure which communicates to the STM\PRV FC (1,2,6)	59
6.16.4	FC Failure to OASyS (Web Services Interface) (2,4)	59
6.16.5	Malformed Report (Web Services Interface) (2)	60
6.16.6	STM FC Failure to PRV FC (3)	61
6.17	Failure of Reporting Server.....	62
6.17.1	Failed Component and Description of Failure	62
6.17.2	Impact on Operations / System and Severity	62
6.17.3	Typical Cause of Failure.....	62

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 9 of 68

6.17.4

Means of Detection and Controls.....

62

6.17.5

Rectification and Impact of Rectification

62

6.17.6

Preventative Maintenance.....

63

6.18


Islanded Operations.....

64

7

APPENDIX A – REALTIME PROCESSES

65

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 10 of 68

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to:

- Describe the redundancy built into the Transnet Pipelines' OASyS DNA system and the interface to the PLCs/RTUs (e.g. Flow Computers). The primary objective is to mitigate the impact on failure modes.
- Identify and analyse the Failure Modes of the OASyS DNA SCADA system and the interface to the PLCs/RTUs.
- Define recovery actions for each of the failure modes identified.

This document is the guiding document for reliability calculations of the system.

This document also supports how the PCS Mean Time Between Failure (MTBF) is calculated.

1.2 Scope

1.2.1 Requirements Included

This document provides detailed calculations, as they relate to the SCADA. This document is intended to provide detailed examples of the hardware and software components and calculations. This document describes the redundancy and transfer mode mechanism for Transnet Pipelines which a system administrator can define and utilize on the SCADA.

In this document, SCADA includes LMS and LDS applications.


1.2.2 Requirements Excluded

This document does not cover the failure modes outside of the PCS SCADA Layer i.e. PLC and Flow Computer sub-systems. Field wiring and IO are also omitted.

1.3 Terms and Definitions

1.3.1 Abbreviations

Term	Definition
ACE	Advanced Calculation Engine
ADE	Advanced Database Editor
AOR	Area of Responsibility
AT	Acceptance Testing
BLT	Business Logic Tier
DC	Domain Controller
DNA	Dynamic Network of Application
DSS	Decision Support Services
LDS	Leak Detection System

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 11 of 68


Term	Definition
LMS	Liquid Management Suite
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
OASyS	<u>O</u> pen <u>A</u> rchitecture <u>S</u> yStem
PLC	Programable Logic Controller
RDBMS	Relational Database Management System
SCADA	<u>S</u> upervisory <u>C</u> ontrol <u>a</u> nd <u>D</u> ata <u>A</u> cquisition
SSRS	Microsoft <u>S</u> QL <u>S</u> erver <u>R</u> eporting <u>S</u> ervices
T&D	<u>T</u> est and <u>D</u> evelopment environment
NSA	Network Security Appliance (Firewall)

Table 1.1: Abbreviations


1.3.2 Definitions

The following definitions apply for this document:

Definition	Description
Advanced Database Editor (ADE)	An OASyS DNA support and configuration program for editing the real-time database.
Availability	The probability that a system will perform its designed function when required to do so is expressed as the fraction (or percentage) of time a system or individual module remains on-line and performs as specified during an observation period. It is calculated as follows: $A = MTTF/MTBF$ or $A = MTTF/(MTTF + MTTR)$
Control Panel	A standard graphic element that represents a telemetered value, for example, an analogue controller instrument, a hardwired push-button, or a switch, allowing operator monitoring and control of the device.
Display	Graphics which will show the information coming from the RealTime database statically or dynamically.
Fault Tolerance	The property of a system which permits it to carry out its assigned function even in the presence of one or more faults in its hardware or software components. Fault tolerance is to be achieved automatically without any user intervention
FC	Stream and Prover Flow Computers, used for custody volume measurement.
HMI	The graphical interface program for allowing an operator to interact with and control a process

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 12 of 68

Definition	Description
MTBF	MTBF is the expected time between failures of a system including the time to repair. It is derived in its simplest form as: $MTBF = MTTF + MTTR$
MTTF	MTTF is the expected time to failure of a system in a population of identical systems
MTTR	MTTR is the statistical average of time taken to identify and repair a fault (including diagnostics)
Mode	Control block operational condition, such as manual, automatic, or cascade
Monitor	A physical device used to show displays.
Operator Workstation	Electronic equipment on which the HMI resides, including, at a minimum, PC workstation, a monitor, keyboard, and pointing device used by an operator to monitor and control his assigned process or manufacturing units
Operator / Controller	One who exercises central surveillance and control of the field using SCADA.
PLC	Programmable Logic Controller, used for discrete and continuous control in processing and manufacturing plants
Point	A process variable derived from an input signal or calculated in a process calculation
Real-time	The inherent property of a system to distribute data such that the users of the data always have the most current data at all times.
Reliability	The probability that when operating understated environmental conditions, the system will perform continuously, as specified, over a specific time interval
Redundant	A system/subsystem with two modules that provides automatic switchover to a backup in the event of a failure, without loss of a system function
Screen	Part of the monitor is shown to arrange displays.
System Software	The software components that are required to make the system functional and fit for purpose. System software shall include any firmware, operating software and tools that are supplied as standard items (for example configuration software, operating system and human interface configuration software). Typically, the system software is configured to meet user requirements


TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 13 of 68

2 APPLICABLE DOCUMENTS

All documents of the exact revision cited in the Applicable Documents form part of this specification to the extent specified. In the event of a conflict between the text of this specification and the documents invoked herein, the text of this specification takes precedence. Nothing in this specification supersedes applicable laws and regulations.

2.1 TPL Applicable Specifications and Standards

No. and Title	Doc. No.	Rev.
[1] SCADA Functional Design Specification	E354086-00000-271-078-0018	Latest
[2] PLC Functional Design Specification	E354086-00000-271-078-0003	Latest
[3] Metering Functional Design Specification	E354086-00000-271-078-0020	Latest
[4] SCADA / PLC Communication Plan	E354086-00000-271-078-0012	Latest
[5] LDS Functional Design Specification	E354086-00000-271-078-0007	Latest
[6] LAN Specification	E354086-00000-271-078-0002	Latest
[7] PCS Control Module Specification	E354086-00000-271-078-0005	Latest
[8] SCADA System Architecture	E354086-00000-271-256-0002	Latest
[9] PLC System / LAN Architectures	E354086-00000-271-256-0003, 0004, 0005, 0006	Latest
[10] PCS Performance Specification	E354086-00000-271-078-0014	Latest
[11] Process Control System User Requirement Specification	TPL-TECH-I-C-SPEC-012	03
[12] Process Control System Software Control Module Standard	TPL-TECH-I-M-SPEC-013	01
[13] Custody Metering System User Requirement Specification	TPL-TECH-I-M-SPEC-011B	04
[14] Leak Detection System User Requirement Specification	H354086-00000-270-078-0004	0
[15] Replay System User Requirement Specification	H354086-00000-270-078-0003	0
[16] HMI Trainer System User Requirement Specification	H354086-00000-270-078-0002	0
[17] Transnet Pipelines WAN – Crude Oil Pipeline Automation Systems LAN ICD	H354086-00000-276-242-0001	0
[18] PL703 Process Control Network Standard	PL703	2.0
[19] Pipeline Network Design Criteria	2684358-J-A00-CS-SP-001	04
[20] PCE – Framework for Minimum Controls for Security	TPL TECH MC&I STD PCE-006	2.0
[21] Control – Vulnerability and Firewall Configuration Management	TPL-TECH-C-WI-001	01

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 14 of 68

No. and Title	Doc. No.	Rev.
[22] Computer Naming Standard	2684358-S-A00-IS-ST-001	04
[23] Alarm Philosophy	H354086-00000-270-080-0001	B
[24] Alarm Configuration Database	H354086-00000-271-060-0001	Latest
[25] S600 Flowboss Stream Functional Design Specification	TPL-TECH-I-M-SPEC-016	R4
[26] S600 Flowboss Prover Functional Design Specification	TPL-TECH-I-M-SPEC-017	R4
[27] PLC System Architecture Failure Analysis	E354086-00000-271-078-0016	Latest
[28] Network Diagnostics Specification	E354086-00000-271-078-0026	Latest

2.2 Other Applicable Specifications and Standards


The following national and international standards are complied with and can be read in conjunction with this specification.

No.	Doc. No.	Rev.
[29] Nil.		

2.3 Reference Documentation

The documents included in this section do not form part of the specification but are included for background and context.

No.	Doc. No.	Rev.
[30] Nil.		

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 15 of 68

3 TPL SYSTEM

3.1 System Availability

The overall PCS System availability has been calculated using the PLC Availability figures [27], and the dominant SCADA availability scenario (Fallback PLC polled from MCC). The scenario below indicates that the compliant MTTR for the TPL Crude Oil Pipeline is 24hrs.

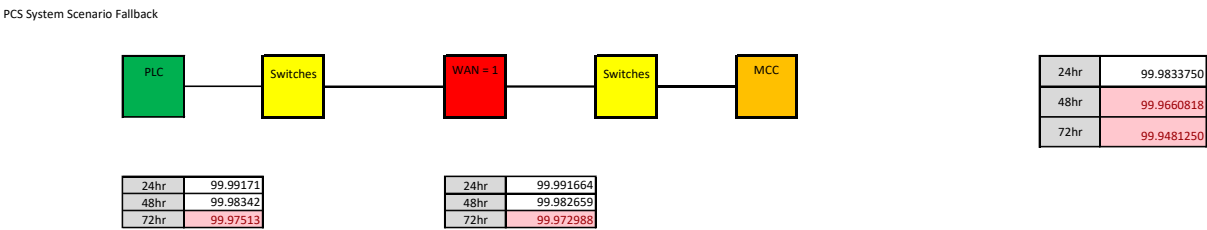


Figure 3-1 – PCS System Availability

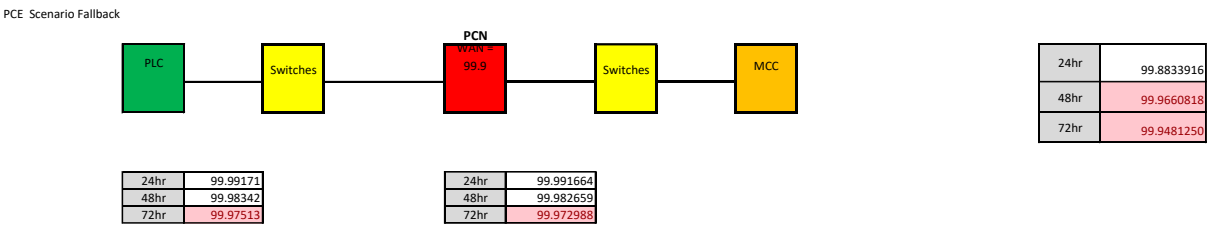


Figure 3-2 – PCE Availability

3.2 System Architectures

The architecture for the Transnet Pipelines’ SCADA System is based on three levels for data acquisition and processing:


- 1) Station (STN) SCADA: Primary owner of data acquisition processing (for example alarm limit checking) and local operations control;
- 2) Master Control Centre (MCC) SCADA: Secondary data acquisition, data processing, remote control, centralized data configuration, and CMS and LDS integration; and
- 3) Decision Support System (MCCDSS): Integration environment for the exchange of data outside of the OASyS SCADA network.

These three levels of data acquisition and processing ensure the availability and performance required for the operation of the Transnet pipeline network, with the highest levels of security and maintaining of data integrity across the system. Each one of the levels includes services for the processing of real-time and historical data.

The architecture is based in the approved Reference Architecture of OASyS DNA [8] for the management of crude oil and multi-product pipelines.


The main design criteria of the Transnet system architecture include:

- Redundancy and Availability;
- Functional Separation; and

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 16 of 68

- Ability to Meet Performance

The sections below detail the different aspects of the solution and elaborates how the solution addresses these design criteria.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 17 of 68

3.3 Physical Architecture

The architecture is based on a physical virtual host and virtual guest servers. Specified for each virtual guest in the system, are its included Identifier, Services and Licenses and required Memory, CPU, and Storage.

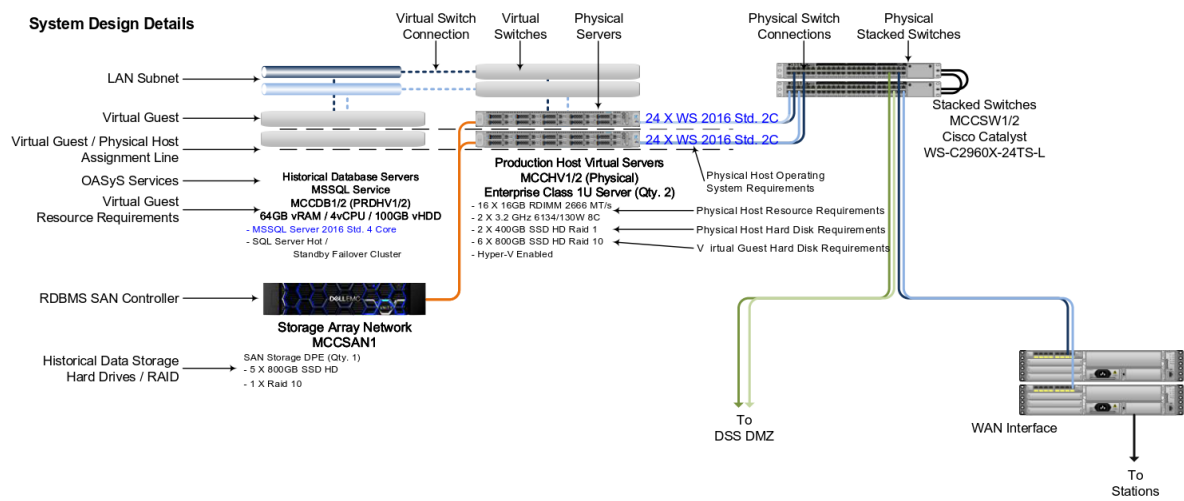



Figure 3-3 – Redundant Virtual Guest / Physical Host Server Design

3.4 System Architecture

The schema below is a simplified diagram of the architecture of the MCC SCADA, CMS, and LDS system.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 18 of 68

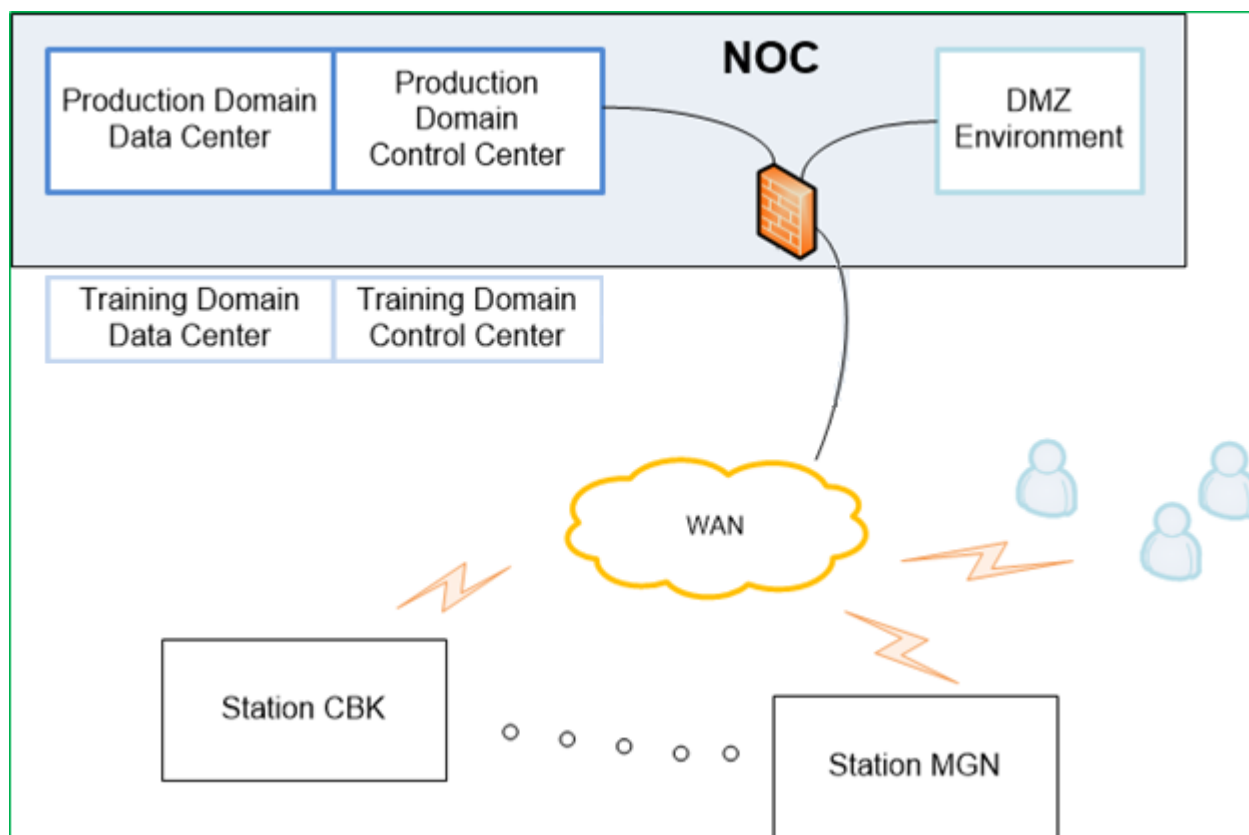



Figure 3-4 - MCC Architecture


The MCC is divided into two separate zones:

- 1) Production Domain, which is the critical infrastructure of the system and includes:
 - a. Redundant Domain Controllers (one physical);
 - b. Redundant Hot / Standby SCADA (RealTime, Historical, and Archive Services) servers;
 - c. Redundant Historical Database servers;
 - d. Liquids Management System, including CMS functionality;
 - e. Redundant LDS servers;
 - f. Remote access server;
 - g. Engineering (Deployment) server with SCADA and LDS tools;
 - h. Support server for playback, antivirus and logging; and
 - i. Workstations for the operation of the SCADA, LMS, and LDS;
 - j. Workstations for the engineering of the SCADA, LMS, and LDS.
- 2) Decision Support (DMZ) domain, that includes a host virtual server and virtual machine containing SCADA and LMS data used for integration and exchange of data without affecting the critical infrastructure.
- 3) Temporary interface to ATMOS PIPE LDS will be done via OPC within DSS server.
- 4) AVEVA will test for compliance of the Windows and Antivirus updates and notify clients which updates are approved for use. TPL can download the Windows and Antivirus updates from respective sites and manually roll out to the OASyS system in the production environment.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 19 of 68

The Training Centre at Pinetown will be provisioned with a Training System:

- 1) Training Domain, which includes the HMI Trainer system will reside separately with no network connection to other systems.

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 20 of 68


3.5 Coalbrook (CBK) Intake/Delivery Station Architecture

Coalbrook Station has a local redundant architecture, which caters for three pipelines; Crude, Multi-Product and Avtur. The Coalbrook delivery station is manned 24/7 and locally operated.

All Pipeline systems on Coalbrook have custody metering installed.

The Coalbrook Station will be provisioned with the following components:

- Local Domain Controller;
- Redundant Hot / Standby SCADA (RealTime, Historical, and Archive Services) services;
- Redundant RDBMS servers;
- Redundant Historical Database servers;
- Liquids Management System, including CMS functionality (refer Metering FDS [3] for details);
- Engineering server with SCADA tools;
- Dual Workstations for the operation of the SCADA and LMS.


TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 21 of 68

3.6 Fynnlands (FYN) Intake Station Architecture

Fynnlands Station has a local redundant architecture, which caters for the intake of crude into the COP pipeline. The Fynnlands intake station is manned 24/7 and locally operated.

The Fynnlands Station will be provisioned with the following components:

- Local Domain Controller;
- Redundant Hot / Standby SCADA (RealTime, Historical, and Archive Services) services;
- Redundant RDBMS servers;
- Redundant Historical Database servers;
- Liquids Management System, including CMS functionality (refer Metering FDS [3] for details);
- Engineering server with SCADA tools;
- Dual Workstations for the operation of the SCADA and LMS.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 22 of 68


3.7 Pump / Booster Station Architecture

These stations will have a local non-redundant architecture with the MCC providing Standby Services.

These stations will be provisioned with the following components:

- Local Domain Controller;
- SCADA Server (RealTime and Historical);
- Historical MS SQL Service;
- HMI server, with SCADA engineering tools; and
- Workstation for SCADA operations.

For CBK, FYN, Pump and the booster stations, the HMI server includes all the functions for the visualization/operation and the editing / modifying of displays. The Operator Workstation can connect to the local servers or the Remote Access Servers at the MCC in case of failure of the local servers.

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 23 of 68

4 SYSTEM AVAILABILITY

4.1 Availability Considerations

The OASyS DNA Solution is comprised of the hardware that provides the platform for the SCADA system and the software that provides the infrastructure and the SCADA functionality. These components are considered for availability estimation.

A key element that enhances the overall system Availability is the OASyS DNA redundancy model, as described in the SCADA Functional Design Specification [1]. If the machine; power supplies, hard drives, and NIC ports or a critical component fails, a redundant pair component is ready to assume the function, which allows the system to continue providing that functionality while a maintenance action is taken to restore the failed each Host Virtual server, redundant controllers and pairs of RAID 1 physical disks for each application module in the SAN disk enclosures.

Other devices not critical to the SCADA operations, such as printers, are not included in the System Availability calculations.

4.1.1 Redundant LAN Network

4.1.1.1 MCC

Redundant switches, A and B will be installed using stacked configuration. All devices excluding GPS Network Time Server, UPS and Network Printers will be supplied with 2 network cards. Each device with dual network cards will be connected to Switch A and Switch B.

4.1.1.2 Coalbrook and Fynnlands

Redundant switches, A and B will be installed using stacked configuration. All devices excluding Network Printers and Flow computers will be supplied with 2 network cards. Each device with dual network cards will be connected to Switch A and Switch B.

Flow computers are interfaced to the SCADA using Switch A. A backup cable is wired in, should a failure happen. In this case the wire has to be plugged in by a technician.

Note that printing from the FC is assigned to a single ethernet port.


4.1.1.3 Pump and Booster pump stations

Redundant switches, A and B will be installed using stacked configuration. All devices excluding Network Printers will be supplied with 2 network cards. Each device with dual network cards will be connected to Switch A and Switch B.

Refer to the LAN Specification [6] and SCADA System Architecture Drawing [8]

4.2 Software Redundancy

The OASyS DNA redundancy model (including LMS and LDS) is self-monitoring with critical functions and devices under constant evaluation as to their availability. This is a key requirement for system robustness and ease of support and administration. Automated monitors will check all critical components for failures and take the least disruptive course of action to recover from any disruption or failure. This redundancy is implemented at both hardware and software levels.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 24 of 68

4.3 Availability Formulas

The Availability (A) of an individual component or device is calculated by the following formula:

$$A = \frac{MTBF}{MTBF + MTTR}$$

Symmetrically, the Unavailability (U) of an individual component or device is calculated by the following formula which is the inverse of the Availability:

$$U = 1 - A$$

The system Availability is calculated based on the network model connections between blocks depending on if they are connected in series or parallel (redundant) configuration. The general the equation for calculating the Availability of a series system (As) of n components is:

$$A_s = A_1 \times A_2 \cdots A_n$$

$$= \sum_{i=1}^n A_i$$

The general equation for the Availability (A) of a parallel system (Ap) of n components is:

$$A_p = 1 - (1 - A_1)(1 - A_2) \cdots (1 - A_n)$$

$$= 1 - \sum_{i=1}^n (1 - A_i)$$

The total availability calculation incorporates the parallel system (Ap) calculation for both the Primary and Secondary SCADA Data Centres. The total availability (At) can be expressed in the availability of these two independent parallel systems (App = Primary Data Centre, Aps = Secondary Data Centre):

$$A_t = 1 - (1 - App) \times (1 - Aps)$$

4.4 Component Reliability and Availability

The following table shows the estimated Reliability and Availability for each critical component required for the operation of the SCADA solution.


TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 25 of 68


Table 4.1 Reliability and Availability Summary

Component (Make / Model)	MTBF (hrs)	MTTR & Availability (%)					
		MTTR (hrs)	Avail- ability (%)	MTTR (hrs)	Avail- ability (%)	MTTR (hrs)	Avail- ability (%)
**Virtual Host server LENOVO SR650	107,494	24	99.977678	48	99.955366	72	99.933064
**Workstation	20,000	24	99.880144	48	99.760575	72	99.641291
*Switch Cisco C9200L-24T-4G-E	531,030	24	99.995752	48	99.991504	72	99.987256
*Router / Firewall Fortinet FG-100F	80,523	24	99.970204	48	99.940425	72	99.910664
**SAN DE2000H	300,000	24	99.992001	48	99.984003	72	99.976006
***OASyS DNA Software All Installations	14,882	24	99.838991	48	99.678500	72	99.518523

* Cisco-provided – on Cisco product datasheet (ref: catalyst-2960x-48lps-l)leno

** Estimated

*** Based on OASyS DNA Critical System Failure (CSF) reporting

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 26 of 68

4.5 Production System Availability

4.5.1 Primary Production System Availability

$$A_s = A_1 \times A_2 \cdots A_n$$

$$= \sum_{i=1}^n A_i$$

The following illustrates the MCC Systems availability where:

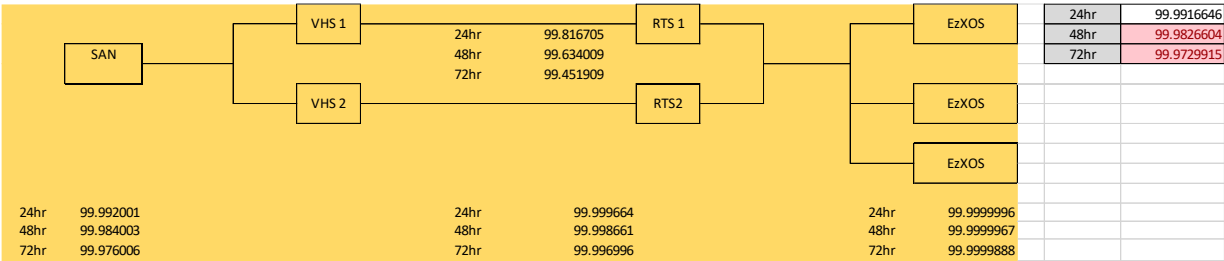


Figure 4-1 – MCC Reliability Block Diagram

4.5.2 Primary Station System Availability

The following illustrates the CBK and FYN Station Systems’ availability where:

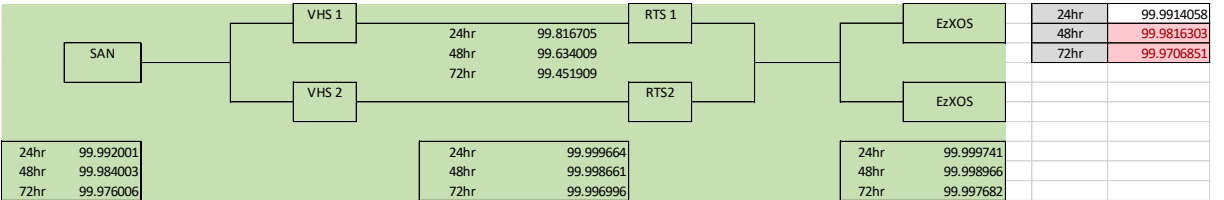


Figure 4-2 – CBK\FYN Reliability Block Diagram

The following illustrates the Pump /Booster station availability where:

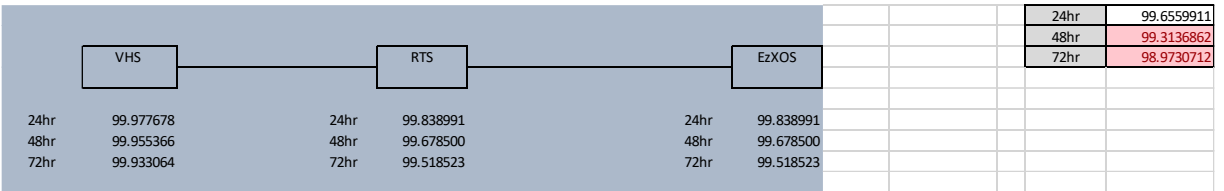



Figure 4-3 – Pump\Booster Reliability Block Diagram

4.6 Total Production System Availability

The total system availability is calculated using the availability of both series and parallel system formula using the Production and Station systems availability calculations from the previous section.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 27 of 68

Scenario 1 to 3: CBK\FYN

- The following device/system availability figures have been used for the SCADA Availability scenario calculations:
 - PLC = 1
 - FC = 1
 - WAN = 1

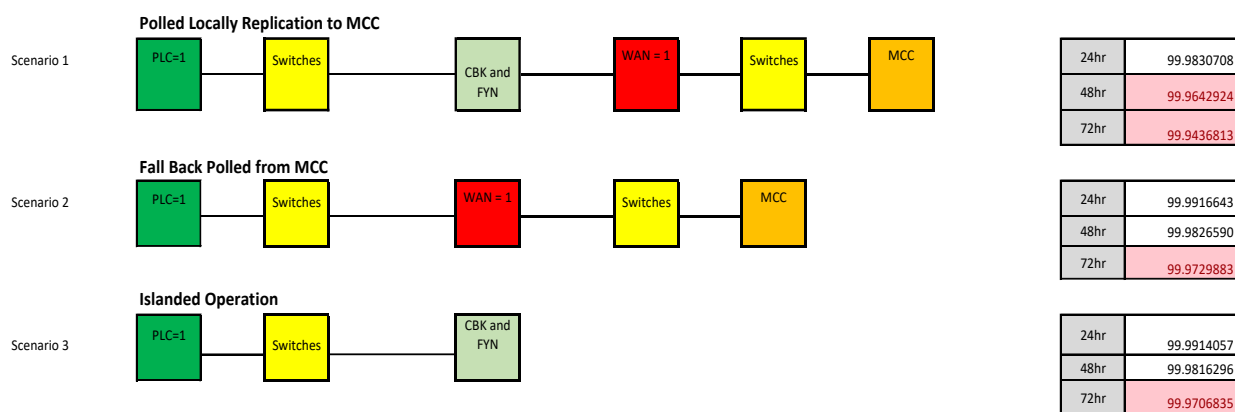


Figure 4-4 – CBK\FYN Operation

Note: Scenarios 1 and 2 are in parallel as the 2nd scenario is the backup to the local polling. If this is done, the answer is the same as for Scenario 2 (WAN in Parallel to the Station SCADA). Therefore Scenario 2 should be used for the MCC availability figure.

Scenario 4 to 6: Pump / Booster Station

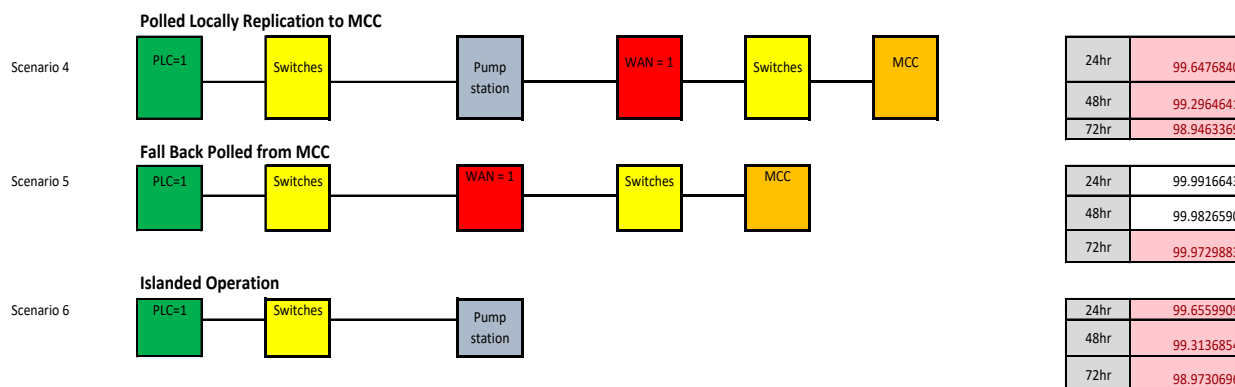


Figure 4-5 – Pump Station Operation

Note: Scenarios 4 and 5 are in parallel as the 5th scenario is the backup to the local polling. If this is done, the answer is the same as for Scenario 2 (WAN in Parallel to the Station SCADA). Therefore Scenario 2 should be used for the MCC availability figure.

Scenario 7: Flow Computer to CBK\FYN



TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 28 of 68



Figure 4-6 FC at CBK\FYN Local Operation

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 29 of 68

5 FAILURE PROTECTION

5.1 Overview

The OASyS system provided to TPL is designed such that there is no single point of failure that can render the system inoperable and lead to loss of control of the pipeline. The system has hardware and software redundancy and mechanisms to continually monitor the health of the system.


Failure protection features include:

- No single point of failure will cause a loss of control of the pipeline; Note: This is true with some clarifications.
- Self-monitoring of PCS equipment;
- Critical software task monitoring;
- Declaration of Service failure, failover and restore;
- Minimal failover time – some failures have a longer fail over time. These have been declared in this document;
- Seamless transfer for Controllers (i.e. no requirement to log off and log back on after a Service failover);
- Alarm and event logs to track failures; and
- The ability of the authorized user to manually trigger a Service failover.

The Hot / Standby configuration for the RealTime, Historical and RDBMS Services facilitates host failure protection through constant communication.

The RealTime hosts in OASyS continually exchange the following information:

- Pulse broadcast - all RealTime hosts in OASyS broadcast their state on the SCADA LAN;
- Automatic RealTime database updates - automatic updates take place for data that are relatively static such as the name of a record;
- Demand RealTime database updates - demand updates (immediate) takes place for significant non-repeatable events (such as an alarm summary record); and
- Periodic RealTime database updates - periodic updates take place for data that will change often (such as an analogue value).

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 30 of 68

5.2 OASyS Services


5.2.1 OASyS Service Failure

If a Hot OASyS Service fails or is not reachable, OASyS automatically transfers control to the redundant Standby Service in a seamless manner. In case the standby system is in a failed state, the failover will not take place. Alarms and events are generated on Service failure, switchover and restore.

Note: This is not applicable to the redundant SQL Server Reporting Services (SSRS) as it is not controlled by OASyS services. SSRS is failed over manually from the SCADA HMI interface by a user with the applicable user rights. Refer to section 6.17.

5.2.2 OASyS Station Failure

In addition to in Site Service failover, there is also an authorized user-initiated switchover between the Master Control Centre (MCC) and each local Station. The MCC can establish communications to the PLCs / flow computers and operations can continue. A user initiated action will mode switch the site back to the Station.

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 31 of 68

5.3 OASyS DistribuSyS and Modes


5.3.1 Overview

OASyS DistribuSyS supports multiple modes of operation where specific modes provide automated failure modes and others are used for manual failure modes (the operational modes). The modes are configurable to allow great flexibility in setting up all the modes to address Transnet Pipelines' needs.

OASyS DNA SCADA has an embedded System Monitor which will detect system failures or violation of defined limits on resource usage. The system monitor has the capability to automatically cause a service to failover.

All OASyS service failovers, as well as manual changes in the failure or operational modes, are alarmed and audit trails of manual service/mode changes are recorded.

Failure conditions and the "Defined Failure Modes" are illustrated below.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 32 of 68

5.4 Failure Modes

5.4.1 Redundant Station SCADA Service Failure

In case of failure of the RealTime or Historical Hot Service in the Station SCADA, for those stations that have Redundant Station SCADA servers (for example Coalbrook), the Station SCADA Standby Service will automatically take ownership of the data acquisition and will continue replicating data to the other Systems. The HMIs at the Station will switch to the new "Hot" Service without affecting the system operation.

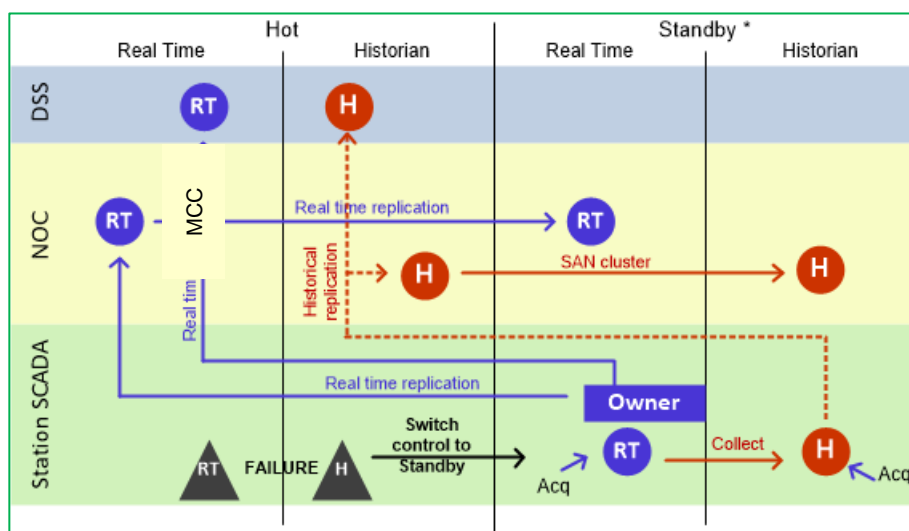



Figure 5-1 – Redundant Data Flow Station SCADA Failure

5.4.2 Non-Redundant Station SCADA Service Failure

In case of failure of a RealTime or Historical Hot Service in the Station SCADA, for those stations that have non-redundant Station SCADA Services (all except Metering Stations), the acquisition for the failed Station will be manually mode switched to the MCC, it will then communicate directly with the PLCs and FCs. The MCC acts as a Redundant system for those Stations. The HMI at the Station can be connected to the MCC System, allowing for control from the Station.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 33 of 68

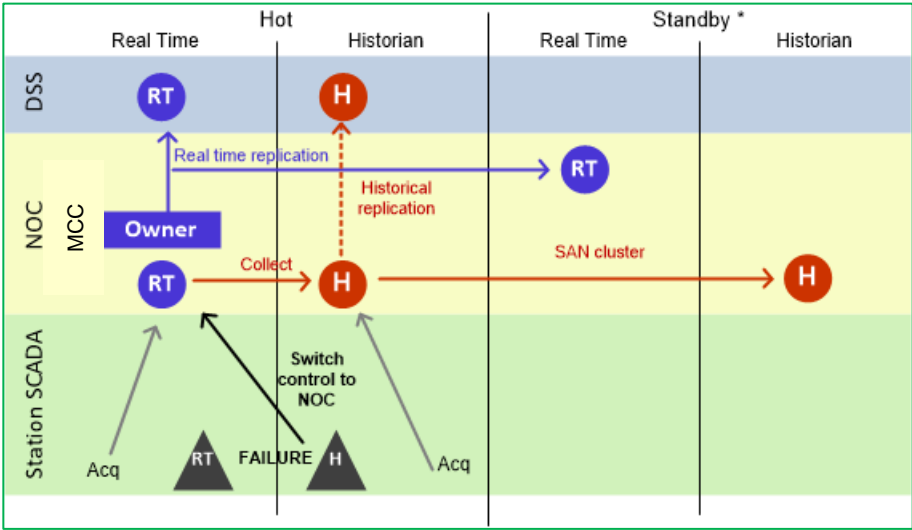



Figure 5-2 – Non-Redundant Data flow under Station SCADA failure

After the failure of the Station SCADA is resolved and the Station SCADA is returned to service, the system will perform an integrity update and replicate from the MCC to the Station SCADA the current information. A manual mode switch to the Station will re-enable local data acquisition.

OASyS will utilise the Network Management Console to monitor the status of the OASyS services.

5.4.3 Non-Redundant Station Workstation Failure

In case of failure of a workstation in the Station SCADA, for those stations that have non-redundant workstations, a failed device alarm and event will be generated at the Station and MCC. After the workstation is repaired and brought back online a return to normal alarm and event will be generated at the Station and MCC.

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 34 of 68

5.5 Limited or Complete Loss of Communications

The OASyS DNA SCADA system has been designed to manage complex geographically distributed pipeline networks, ensuring the availability and continuity of the operations and the data integrity with significant tolerance to communications failures.

The Transnet Pipelines architecture includes redundant LANs at remote Stations and at the MCC and can manage multiple WAN routes for the communications between the Stations and MCC.

The temporary loss of communications between subsystems is a normal problem in geographically distributed networks.

The temporary loss of communications may affect communication between the Station SCADA and the field equipment and between the Stations and the MCC.

5.5.1 Loss of Communication with Field Equipment

The OASyS SCADA system supports multiple communication routes with each PLC and Flow Computers (where installed). If PLC/FC data acquisition is interrupted and cannot be established through either communication line, the Station SCADA system will alarm, event and set the corresponding quality flags associated to the data readings of that PLC/FC to "stale". This is used to notify other applications, for example, the CMS or LDS systems, that the points associated with that PLC/FC are not valid for calculations.

Once the communication with the PLC/FC is re-established RealTime replication will once again transfer values to the other Systems. The SCADA system will alarm and event when communications are restored.


In the case of flow computers, redundant communications are routed through a single switch, resulting in a single point of failure.

Indicators are provided showing good, failed, synchronizing and synchronized connections.

5.5.2 Loss of Communication between Station and MCC

Communications may be lost temporarily between a Station and the MCC (longer-term loss of communication is described in the following section). An alarm and event will be generated at both the MCC and the Station, notifying the Pipeline Operator of the condition and the Station SCADA will continue operations normally. Once the communication is re-established, the DistribuSyS function will synchronize the databases between the Station SCADA and the MCC. A return to normal alarm and event will be generated at the Station and the MCC.

When the MCC loses communication with a site the system takes 60s for the MCC to indicate the loss of communication with the Stale Icon. On recovery, it typically takes 30s to recover from stale and resynchronise. Note: Any loss of communications, even 5s causes a loss of 30s.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 35 of 68

6 FAILURE AND RECOVERY

6.1 Network Interface Card (NIC) Connection Failure

Dual-port NIC card - Each dual redundant OASyS System server and the individual workstation are equipped with a dual-port Intel NIC. Each port plugs into one of two stacked switches.

6.1.1 Single NIC Connection Failure

6.1.1.1 Failed Component and Description of Failure

Failure of a NIC connection does not cause any OASyS Service failure and server is not isolated. Workstations operate normally.

6.1.1.2 Impact on Operations / System and Severity

Operations are not affected since systems are set up with dual-port NIC cards.

6.1.1.3 Typical Cause of Failure

- A single port failure on the switch;
- Cable unplugged; or
- A single switch failure.

6.1.1.4 Means of Detection and Controls

OASyS SCADA system alarm and event generated. Windows Management Instrumentation (WMI) is configured to provide feedback on NIC port failures.

The servers and workstations are monitored by the diagnostics tool for failures.

6.1.1.5 Rectification and Impact of Rectification

Reconnect/replace the cable or restart failed port on NIC.

6.1.1.6 Preventative Maintenance

Dual ports minimize maintenance and allow failure on a port to occur without any downtime.

6.1.2 Dual NIC Connection Failure

6.1.2.1 Failed Component and Description of Failure


Failure of both NIC connections causes server isolation and system or site isolation depending on the type of server. This is a rare and unhealthy situation and during this time period, each of the dual servers could become HOT as there is no awareness of its partner. During the time at which both servers are HOT, a SCADA arbitration process attempts to restore stability by assessing the situation and eventually forcing one of the servers to go Standby.

The server which is still connected to the network will provide services and data for the system.

6.1.2.2 Impact on Operations / System and Severity

If a single server has failed, the server which is still connected to the network will continue to provide services to the rest of the system.

Where RealTime and Historical services reside on the server with both NIC ports failed, synchronization of RealTime data and Historical data is not possible. Control of field devices

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 36 of 68

will not be possible from these servers and a failover or mode switch will have occurred to continue and maintain control of the SCADA system. The data that the two servers represent and control cannot be trusted during this failure time period and operations need rectify failures and await for SCADA arbitration or perform a modeswitch if system setup allows for such a scenario.

Note that as the server still has communication to the SAN, the archive will remain on the original HOT server and not switch over as the failure on the SAN level has not been detected. The solution to this is to shutdown\switch the failed server to get all services to switch.

Workstations will become isolated from the servers and not be usable. Sites which have metering/local operations are supplied with two workstations to mitigate this failure.

6.1.2.3 Typical Cause of Failure

- Dual-port failure simultaneously on the NIC;
- Cables connecting to the two NIC ports are unplugged or damaged simultaneously; or
- Two different switches affecting both NIC ports simultaneously fail.

6.1.2.4 Means of Detection and Controls

Workstations communicating to the isolated server indicate a loss of communications. Alarms and logged events are generated by all other services within the SCADA system that communicate with this isolated server.

As indicated, the archive will stop working under these circumstances as they SAN has not switched over.

Windows Management Instrumentation (WMI) is configured to provide feedback on NIC port failures.

6.1.2.5 Rectification and Impact of Rectification


Normal operation in the alternate server\workstation should be possible.

If the mode switch is available that allows for the alternate system to monitor and control the data then perform mode switch as soon as reasonably possible.

Reconnect/replace the cable, replace faulty NIC or faulty switches and allow for SCADA arbitration process to stabilize system before returning mode to the failed system.

6.1.2.6 Preventative Maintenance

Regular diagnostic checks on NIC interface and switches as well as checking of Windows event logs regarding NIC related warnings and errors. Loss of communications or visibility to field devices can be detrimental to operations

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 37 of 68

6.2 Local Area Network (LAN) Switch Failure

LAN switches are stacked, connected with interconnects for firmware and power. Communications with field PLCs such as monitoring and controlling from the SCADA system is a critical task which must be readily available

6.2.1 Single Switch Failure

6.2.1.1 Failed Component and Description of Failure

One of the switches in the stack is powered off or fails.

6.2.1.2 Impact on Operations / System and Severity

SCADA system OASyS Services are not affected by a single switch failure.

6.2.1.3 Typical Cause of Failure

- A switch failure connecting OASyS servers within a site; or
- Loss of rack power.

6.2.1.4 Means of Detection and Controls

OASyS SCADA system alarm and event generated indicating degraded communications path for critical service recoveries such as mode switches and fail-overs. Windows Management Instrumentation (WMI) is configured to provide feedback on switch failures affecting the LAN connection.

6.2.1.5 Rectification and Impact of Rectification

If failures persist, power-cycle the failed switch or replacing the failed switch.

6.2.1.6 Preventative Maintenance

Dual redundant switches minimize maintenance and allow failure on a switch to occur without any downtime due to the availability of the second switch.

Ensure dual switches are configured; in case a switch fails, the second switch can maintain connectivity within the network.

6.2.2 Dual Switch Failure

6.2.2.1 Failed Component and Description of Failure

Both switches in the stack are powered off or fail.

6.2.2.2 Impact on Operations / System and Severity


The site or set of servers may be isolated. Communications with field PLCs such as monitoring and controlling from the SCADA system are unavailable.

6.2.2.3 Typical Cause of Failure

- Both switches fail simultaneously within a site;
- Loss of rack power; or
- Network outage and failures.

6.2.2.4 Means of Detection and Controls

Windows Management Instrumentation (WMI) is configured to provide feedback on switch failures affecting the LAN connection.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 38 of 68


6.2.2.5 Rectification and Impact of Rectification

The mode switch is used to switch control from failed site to backup/redundant site to minimize impact so that work can be performed on failed switches. Inspect and replace switch cabling and power-cycle switches. If failures persist, replacing the switches.

6.2.2.6 Preventative Maintenance

Prepare preconfigured switches for each site and location so that a failed switch can be immediately replaced.

Ensure dual switches are configured in case a switch fails, the second switch can maintain connectivity within the network.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 39 of 68

6.3 Storage Area Network (SAN) Failure

The SAN delivers consistent and secure data transfer infrastructure with uninterrupted data access to the RDBMS disks.

6.3.1 SAN Component Failure

6.3.1.1 Failed Component and Description of Failure

Failure of a single disk in a RAID group is visible on the SAN panel.

6.3.1.2 Impact on Operations / System and Severity

Operations are not affected since SAN has built-in dual redundant components; power supplies, controllers, fibre connections and hard drives.

Systems with redundant Historical servers can switch control and management of the SAN cluster by failing over the control from one Historical server to the other. When the failed Historical server recovers, the user can use the SAN Cluster Manager to perform cluster failover of the control back to the server.

6.3.1.3 Typical Cause of Failure

- Disk failure on the SAN;
- Fibre Channel failure (disconnect or severed cable); or
- SAN controller failure

6.3.1.4 Means of Detection and Controls

SAN supports SNMP for the diagnostic purpose the San will be monitored by a Network Diagnostic tool. Refer to [28]

6.3.1.5 Rectification and Impact of Rectification

When SCADA fails to persist historical data, and suspect a SAN failure, check power to SAN, and inspect all fibre connections. Monitor the lights on the SAN for any hard disk failures or controller failures.

Utilize the Failover Cluster Manager tool to failover over the SAN cluster control from one Historical service to another. Replace any failed hard drives.

6.3.1.6 Preventative Maintenance


Procedural inspection in the server room of the fibre lines to the SAN and watch for the lights on the disks and the controllers of the SAN.

Use the web interface to obtain diagnostic reports from the SAN on a regular basis.

Periodically perform a user-initiated SAN cluster failover to verify that either Historical services of a partner pair can take control of the cluster when there is a need arises where the Hot Historical server fails and an automatic cluster control failover occurs.

6.3.2 SAN Failure

Inter-site historical replication is provided by a replication process that continually synchronizes historians on the SANs throughout the SCADA system. If operations of persisting historical data to the SAN at an individual location fails, the RealTime Service will continue to write data to its local RealTime server's disk as a form of caching (buffering) so

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 40 of 68

that when SAN recovers, the process will extract the buffered historical data and persist to its SAN.

6.3.2.1 Failed Component and Description of Failure

The total failure of the SAN at MCC, MCCDSS, or Station locations.

6.3.2.2 Impact on Operations / System and Severity

Historical data is used for post-process analysis, its impact is not as severe as RealTime polled data. The system's failsafe of buffered data prevent data lost and the redundancy of historical data being replicated between the systems provides further safeguards to the captured historical data.

Failure of SAN at the Station sites would require a mode switch so that MCC can take control and persist the historical data. Once SAN is restored, replication will synchronize the historical data.

Failure of SAN at the MCCDSS would only affect report generation and potential trends accessed by users outside of the SCADA system. Once SAN is restored, replication will synchronize the historical data.

Failure of SAN at the MCC would have no impact on operations since the Station sites are the primary owner of the data. Any local events generated on MCC will be buffered until the SAN is restored, from which the buffered data will be uploaded and replicated to other historians. Replication of historical data will also synchronize MCC with other SANs.

6.3.2.3 Typical Cause of Failure

- Loss of rack power; or
- SAN software failure

6.3.2.4 Means of Detection and Controls

The SAN has a web interface to access configuration and diagnostics. SCADA does not have an interface to monitor SAN diagnostics. When the Historical Service fails to persist data due to communicates failure to SAN, the SCADA system will provide an alarm and logging event persisted to the local historical server.


6.3.2.5 Rectification and Impact of Rectification

When the SCADA system fails to persist historical data, and a SAN failure is suspected, check power to SAN, and reboot if necessary. Monitor the lights on the SAN for any hard disk failures or controller failures. Replace the failed device.

6.3.2.6 Preventative Maintenance

Procedural inspection in the server room of the fibre lines to the SAN and watch for the lights on the disks and the controllers of the SAN.

Use the web interface to obtain diagnostic reports from the SAN on a regular basis.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 41 of 68

6.4 Virtual Guest Server Failure

6.4.1 Failed Component and Description of Failure

If a Hot OASyS Service fails or is not reachable, OASyS automatically transfers control to the redundant Standby Service in a seamless manner. In case the Standby System is in a failed state, the failover will not take place. Alarms and events are generated on Service failure, switchover and restore.

Failure of a virtual guest server on the host virtual server such as an OASyS RealTime server while the service is Hot causes the Hot service to go into Standby; logs, events, and alarms are generated to inform operations.

When a failure occurs on a Hot MCC RTS Server, a switch to the backup occurs. This causes a resynchronisation of all sites (simultaneous resynchronisation). This typically takes 2:30s but can take up to 6:00. Failures can be caused by a failed critical service (See Appendix A for a list of essential services) or a windows system shutdown.

6.4.2 Impact on Operations / System and Severity

Critical virtual guest servers will have a redundant virtual guest server hosted on a separate host virtual server and the failure will automatically initiate a fail-over of the critical Services; RealTime, Historical, Archive, LDS.

A failed historical server will initiate an automatic cluster failover to the standby historical server so that the SAN cluster can continue to be managed and controlled by SCADA.

When a switch over occurs on an RTS server in the MCC, the system will be blind to the site until the system resynchronises. This can take up to 6:00 minutes. Failure on a station will recover to the standby in 34s.

6.4.3 Typical Cause of Failure

- Loss of rack power;
- Operating System failure;
- Low virtual guest disk space; or
- High virtual guest memory usage.

6.4.4 Means of detection and controls


Performance monitoring provides logs and indications of virtual guest resources. OASyS SCADA system alarm and event generated.

6.4.5 Rectification and Impact of Rectification

Increase physical memory on the host and reallocate and increasing the number of cores on guest VMs.

For systems that have redundancy where the failed Hot server becomes Standby, it will be required of operations to determine the cause of the failure and address the failure. The failed server, when started back up, will be in a Standby state until an operator initiated failover is performed or until a new failure on the currently Hot service occurs which forces a failover.

For systems that do not have redundancy, a mode switch of control may be required to maintain control of the site.


TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 42 of 68

Ensure virtual guests have the latest operating system updates and OASyS updates.

6.4.6 Preventative Maintenance

Review performance monitor reports and check logs on individual guest VMs to ensure memory usage and disk space is available.

Perform periodic failovers on servers and services to ensure that redundant pair can take over control and management of the data.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 43 of 68

6.5 Leak Detection System (LDS) Service Failure

6.5.1 Failed Component and Description of Failure

If a Hot LDS Service fails or is not reachable, OASyS automatically transfers control to the redundant Standby LDS Service in a seamless manner. In case the Standby system is in a failed state, the failover will not take place. Alarms and events are generated on Service failure, switchover and restore.

6.5.2 Impact on Operations / System and Severity

Critical servers will have a redundant Service hosted on a separate host server and the failure will automatically initiate a fail-over for the critical services such as the LDS Service.

6.5.3 Typical Cause of Failure

- Loss of rack power;
- Operating System failure;
- Low virtual guest disk space; or
- High virtual guest memory usage.

6.5.4 Means of Detection and Controls

Performance monitoring provides logs and indications of virtual guest resources. OASyS SCADA system alarm and event generated.


6.5.5 Rectification and Impact of Rectification

Increase physical memory on the host and reallocate and increasing the number of cores on virtual guest.

Ensure virtual guests have the latest operating system updates and OASyS updates.

6.5.6 Preventative Maintenance

Review performance monitor reports and check logs on individual guest VMs to ensure memory usage and disk space is available.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 44 of 68

6.6 OASyS Services Failure

The impact of server failure and critical services is also discussed in Section 6.4.

6.6.1 Failed Component and Description of Failure

If a Hot OASyS Service fails or is not reachable, OASyS automatically transfers control to the redundant Standby Service in a seamless manner. In case the Standby system is in a failed state, the failover will not take place. Alarms and events are generated on Service failure, switchover and restore.

When a failure occurs on a Hot MCC RTS Server, a switch to the backup occurs. This causes a resynchronisation of all sites (simultaneous resynchronisation). This typically takes 2:30s but can take up to 6:00. Failures can be caused by a failed critical service (See Appendix A for a list of essential services) or a windows system shutdown.

See Appendix A for a list of services.

6.6.2 Impact on Operations / System and Severity

Impact on operations/system and severity is dependent on service that failed.

For systems that have redundancy where the failed Hot server becomes Standby, it will be required of operations to determine the cause of the failure and address the failure. The failed server, when started back up, will be in a Standby state until an operator initiated failover is performed or until a new failure on the currently Hot service occurs which forces a failover.

When a switch over occurs on an RTS server in the MCC, the system will be blind to the site until the system resynchronises. This can take up to 6:00 minutes. Failure on a station will recover to the standby in 34s.

In the case of the OPC comms service failure, the interface of field signals into ATMOS PIPE LDS will no longer be available. The Leak Detection System segment affected will be degraded and degradation will be alarmed to the operator on the ATMOS PIPE LDS itself.

6.6.3 Typical Cause of Failure

- Loss of rack power;
- Operating System failure;
- Low virtual guest disk space; or
- High virtual guest memory usage.


6.6.4 Means of Detection and Controls

Performance monitoring provides logs and indications of virtual guest resources. OASyS SCADA system alarm and event generated.

In the case of the OPC comms service failure, the interface of field signals into ATMOS PIPE LDS will no longer be available. The Leak Detection System segment affected will be degraded and degradation will be alarmed to the operator on the ATMOS PIPE LDS itself.

6.6.5 Rectification and Impact of Rectification


Increase physical memory on the host and reallocate and increasing the number of cores on the virtual guest.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 45 of 68

Ensure virtual guests have the latest operating system updates and OASyS updates.

6.6.6 Preventative Maintenance

Review performance monitor reports and check logs on individual guest VMs to ensure memory usage and disk space is available.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 46 of 68

6.7 OASyS Software Application Failure

6.7.1 Failed Component and Description of Failure

A standard OASyS system may include the following services:

- Common – common infrastructure (core application) services
- Arbitration – inter-server arbitration services
- RealTime – real-time data processing service
- ISPS (Inter-System Publish/Subscribe) – inter-system data communications service
- RCS (Remote Client Service) – remote access and control service
- Historical – historical data processing service
- Reporting – report generation service
- Archive – archiving of historical data onto external storage

Within each service, an application that manages critical data can be configured as a critical process such that a serious failure on this process will cause the entire service to failover from the hot to the standby system.

Refer to Appendix a – realtime processes for a detailed list of TPL RealTime processes.

For details of the various services and applications within the OASyS system, refer the SCADA Pipeline Edition Administration Guide [28].

6.7.2 Impact on Operations / System and Severity

Although applications failure can occur within any service and cause a failover of the service as discussed in previous sections, the impact on operations is most prevalent among applications within the RealTime Service.

For example, the LMS application is configured as a critical process due to the importance of the data it manages. This application resides within RealTime Services, so when this application fails, a failover will be triggered to switch the RealTime Service from the hot system to the standby system. The failover will ensure data integrity is maintained and the LMS application can continue to run seamlessly.

6.7.3 Typical Cause of Failure


- The application throws an exception due to fatal errors;
- Application access illegal register addresses; or
- Memory allocation failures.

6.7.4 Means of Detection and Controls

Fatal errors and exceptions will generate a log file within the SCADA host for analysis. Similarly, illegal register and memory access will generate a log file.

6.7.5 Rectification and Impact of Rectification

Failures will cause a hot to standby failover to maintain SCADA data integrity and operations.


TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 47 of 68

Reporting Services failure does not cause an automatic failover of the Reporting Services. Technician level users need to do a manual failover of the Reporting Services failover

Logs generated by application failures due to software errors may be sent to SCADA application developers to be analysed and fix identified.

6.7.6 Preventative Maintenance

Software updates and changes to applications follow coding standards and software development processes. These procedures include testing at various stage of development to reduce deficiencies in software and improve robustness and reliability of applications.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 48 of 68

6.8 Domain Controller (DC) Failure

6.8.1 Failed Component and Description of Failure

A DC is installed on each site along with a backup DC. In addition, all DCs within the SCADA network synchronize the data such as security information, authentication, timing services, and networking information to ensure data integrity within the SCADA system. A failure on any one of the DCs within the system has no impact on the system due to the redundancy.

6.8.2 Impact on Operations/System and Severity

A failure on any one of the DCs within the system has no impact on the system due to the system built redundancy.

6.8.3 Typical Cause of Failure

- Loss of rack power; or
- Low disk space on the host server

6.8.4 Means of Detection and Controls

Performance monitoring provides logs and indications of virtual guest resources.

Windows event logs are persisted and can be assessed post failure.


6.8.5 Rectification and Impact of Rectification

Increase physical memory on the host and reallocate and increase the number of cores for the affected DC.

Force a resync of the DCs or Restarting of the DC.

6.8.6 Preventative Maintenance

Ensure DC has the latest operating system updates and patches. Review performance monitor reports and check logs on individual virtual guests to ensure memory usage and disk space is available.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 49 of 68

6.9 Time Server Failure

6.9.1 Failed Component and Description of Failure

The time server communicates with a GPS time source and if a failure on this server occurs, the referencing devices such as the Domain Controller will free run on its local clock until the time server provides accurate time.

6.9.2 Impact on Operations / System and Severity

A failure of the time server will not affect SCADA time. The DCs will provide local time and synchronize the servers and workstations time until the device is restored.

6.9.3 Typical Cause of Failure

- Loss of rack power
- Communications with GPS is lost

6.9.4 Means of Detection and Controls


Performance monitoring provides logs and indications of virtual guest resources. OASyS SCADA system has no awareness of Time Server failures and alarms and events are not generated.

6.9.5 Rectification and Impact of Rectification

Repair / replace faulty time server.

6.9.6 Preventative Maintenance

Periodic inspection of the time server and GPS connection.

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 50 of 68

6.10 Network Security Appliance (Firewall Failure)

The NSA's installed within the DMZ environment which provides access to outside systems.

6.10.1 Failed Component and Description of Failure

NSA powered off or fails.

6.10.2 Impact on Operations / System and Severity

NSA between DSS and Production

- Loss of data from production to DSS including ticket information on DSS for the corporate interface. Production data will only be available on Production Domain.

NSA between DSS and Corporate

- Loss of data exchange from DSS to Corporate. This implies no ticket information will be available to SAP.

NSA between DSS and ATMOS PIPE LDS

- ATMOS PIPE LDS will not receive any process info and will be inoperable. This implies no leak detection during the transition period.

NSA between DSS and the Internet.

- No DSS connection to the Internet. This will impact remote access, downloading of security updates etc.

6.10.3 Typical Cause of Failure

- NSA equipment failure;
- Loss of rack power; or
- Network outage and failures.

6.10.4 Means of Detection and Controls

NSA between DSS and Production


- OASyS system will detect and alarm that connection to DSS host server is lost, when OASyS replicates data to the DSS server
- NSA will be monitored for failure. SNMP Diagnostic tool will be utilised to monitor device failures [28].

NSA between DSS and Corporate

- Corporate retrieval of production data will not take place
- NSA will be monitored for failure. The diagnostic tool will be utilised to monitor device failures [28].

NSA between DSS and ATMOS PIPE LDS

- ATMOS PIPE LDS will have ALARM loss of info from segments or total loss of process info and go into an alarm state. Corporate retrieval of production data will not take place
- NSA will be monitored for failure. The diagnostic tool will be utilised to monitor device failures [28].

TRANSNET PIPELINES		 TRANSNET pipelines	
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 51 of 68

NSA between DSS and the Internet.

- No internet connection
- Remote login is not possible
- NSA will be monitored for failure. The diagnostic tool will be utilised to monitor device failures [28].

Note: The SMNP monitoring will need to be tunnelled through the firewall as per details given in [28].


6.10.5 Rectification and Impact of Rectification

On failure, the following options exist,

- Replacement of failed equipment
- A reboot of equipment for software failure.

6.10.6 Preventative Maintenance

Ensure software updates and patches are routinely performed on the NSA. Utilize provided a diagnostic tool for the NSA to assess the health of the firewall.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 52 of 68

6.11 Decision Support System (DSS) Failure

6.11.1 Failed Component and Description of Failure

Failure of a DSS server affecting interfaces to the SCADA system and interfaces to business applications.

6.11.2 Impact on Operations / System and Severity

Failure of the DSS' has minimal impact on operations from a business perspective since only reports are generated or hosted on the DSS. DSS contains RealTime and Historical as well as Reporting Services amongst other business interfaces that may be interfacing SCADA such as scheduler applications.

6.11.3 Typical Cause of Failure

- Loss of Rack power
- Operating System failure
- Other non-OASyS application fatal errors

6.11.4 Means of detection and controls

Performance monitoring provides logs and indications of virtual guest resources. OASyS SCADA system alarm and event generated.


6.11.5 Rectification and Impact of Rectification

Assess other non-OASyS applications to ensure resource usage is viable and non-intrusive to co-exist with OASyS. If critical OASyS processes fail, automatic fail-over allows for immediate recovery of OASyS services; however, manual fail-over is available to expedite the fail-over to allow maintenance of failed DSS.

6.11.6 Preventative Maintenance

Review performance monitor reports and check logs on DSS to ensure memory usage and disk space is available, as well as assess other non-OASyS applications and processes.

Ensure DSS has the latest operating system updates and OASyS updates.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 53 of 68

6.12 Workstation Failure

6.12.1 Failed component and description of the failure

Failure of a workstation affecting interfaces to SCADA operator and controller to the SCADA system.

6.12.2 Impact on Operations / System and Severity

Monitoring and controlling SCADA system is a critical task which must be readily available. Any loss of communications or visibility to field devices can be detrimental to operations. All site will have multiple workstation access to the sites to allow for viewing and controlling. This is a built-in design using the AOR (Areas of Responsibility) to ensure all areas have more than a single workstation accessible to a location.

6.12.3 Typical Cause of Failure

- Loss of rack power; or
- Operating System failure.

6.12.4 Means of Detection and Controls

Logged events captured at SCADA level and stored in persistent memory.

Performance monitoring provides logs and indications on workstation resource issues

These alarms will be routed to the engineering environment.


6.12.5 Rectification and Impact of Rectification

If critical OASyS processes fail on the workstation, additional workstations will have access/control/ and visibility of the workstations area of control. Typically, a restart of OASyS processes or reboot of the workstation can recover workstation.

6.12.6 Preventative Maintenance

Review performance monitor reports and check logs on the workstation to ensure memory usage and disk space is available.

Ensure workstation has the latest operating system updates and OASyS updates.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 54 of 68

6.13 Historical Playback Data Capture Failure

6.13.1 Failed Component and Description of Failure

If a Historical Playback data capture fails, process data will not be available for replay.

6.13.2 Impact on Operations / System and Severity

Historical Playback data will not be available for replay.

6.13.3 Typical Cause of Failure

- Loss of rack power;
- Operating System failure;
- Low virtual guest disk space; or
- High virtual guest memory usage.

6.13.4 Means of Detection and Controls

The Playback application will be monitored and alarmed as a critical service.


6.13.5 Rectification and Impact of Rectification

Increase physical memory on the host and reallocate and increasing the number of cores on the virtual guest.

Ensure virtual guests have the latest operating system updates and OASyS updates.

6.13.6 Preventative Maintenance

Review performance monitor reports and check logs on individual guest VMs to ensure memory usage and disk space is available.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 55 of 68

6.14 SCADA System Communication to PLC Failure

6.14.1 Failed Component and Description of Failure

Failure of the communications link between the SCADA system and PLCs in the field.

6.14.2 Impact on Operations / System and Severity

SCADA system to PLC communications is a critical task which must be readily available. Any loss of communications or visibility to field devices can be detrimental to operations. All critical locations will have two (2) physical connections, one to each of the stacked switches.

6.14.3 Typical Cause of Failure

- Loss of rack power; or
- Network outage and failures

6.14.4 Means of Detection and Controls


Alarms and Logged events captured at SCADA level and stored in persistent memory.

6.14.5 Rectification and Impact of Rectification

Network recovery and assessment of connection are required. In some cases, working with the telecommunications department is necessary to resolve communications problems.

6.14.6 Preventative Maintenance

Ensure two connections are configured.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 56 of 68

6.15 SAP Interface Failure (Via DSS)

6.15.1 Failed Component and Description of Failure

SAP interface fails, such that there is a disconnect in communications between the DSS and SAP.

Additional failure can occur on the SCADA side such that SAP cannot get current data from DSS.

6.15.2 Impact on Operations / System and Severity

SAP will initiate (either periodically or on-demand) the connection to the SCADA host DSS on the defined SQL interface and obtain the required data.

If the data is not available for an extended period of time, it may affect upload time as there is a larger buffer of data to retrieve.

6.15.3 Typical Cause of Failure

- Loss of rack power; or
- Network outage/failure.

6.15.4 Means of Detection and Controls

SAP will fail to connect to SCADA host and SQL Queries will fail. Errors are detected on the SAP side.


If the connection is successful, but SQL Queries do not return relevant or current data over an extended period (more than 2 days), SCADA host will provide error logs and events that indicate a failure in replicating data from the stations and the MCC to the DSS.

6.15.5 Rectification and Impact of Rectification

Restart of historical services in accordance to the SCADA host recovery procedures.

6.15.6 Preventative Maintenance

Review SCADA host logs and events to ensure no issues with historical data replication between station to DSS and MCC to DSS.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 57 of 68

6.16 Metering

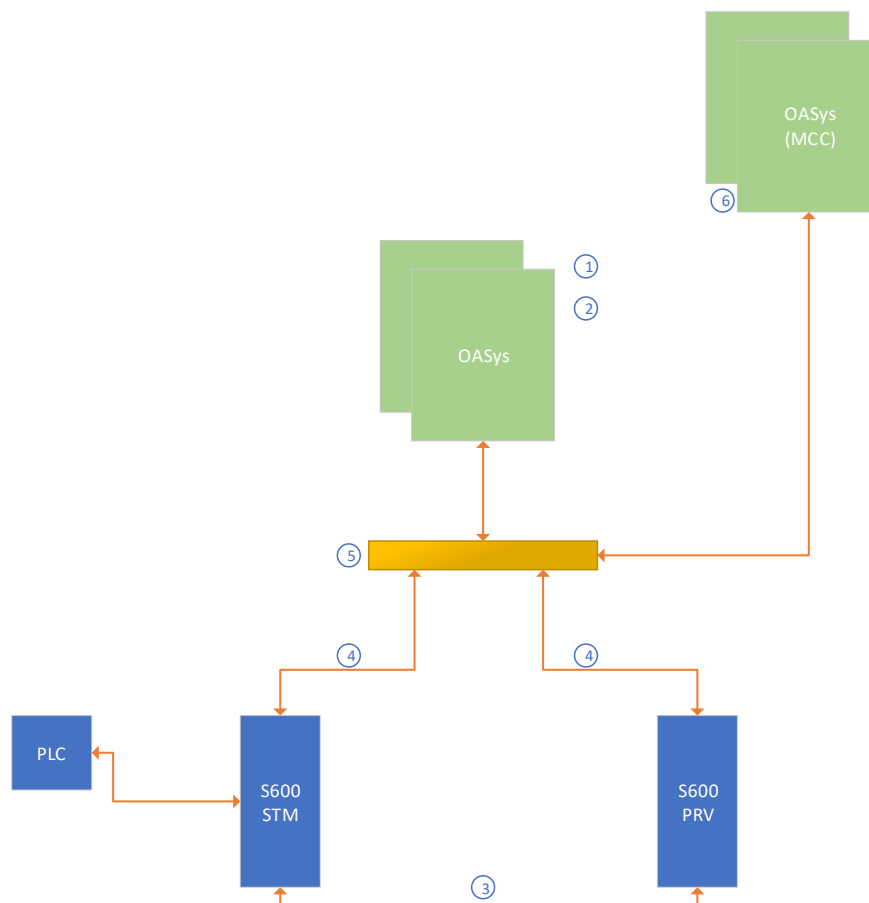


Figure 6-1: Metering Failure Modes

6.16.1 PRV FC Failure to OASys (Modbus Interface) – Total Loss Interface (1,4)

6.16.1.1 Failed Component and Description of Failure

Modbus communications failure between the FC and SCADA host. The network links have failed, or the common stacked switch has failed.

6.16.1.2 Impact on Operations / System and Severity


Database configuration ensures the communications path between the FC and the SCADA host are monitored. An alarm is generated to the operator indicating the fail.

If the prover communication has failed,

- A proof cannot be initiated
- If a proof is in process already, then the proof will complete but the report upload to the SCADA will not work until comms is re-established

6.16.1.3 Typical Cause of Failure

- Cable fault; or
- Network switch failure; or

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 58 of 68

- S600 failure

6.16.1.4 Means of Detection and Controls

SCADA host will provide error logs and events that indicate Modbus failure between FC and SCADA host. Alarms for communications failures with the FC will provide an indication to the operator.

6.16.1.5 Rectification and Impact of Rectification

Check S600, cables and switches for this connection.

Check database point configurations for related remote and connection records to ensure that IP addresses and ports are correct for the specified protocol.

If the port on the S600 has failed, the back-up port can be used.

6.16.1.6 Preventative Maintenance

Check wiring and cables between routers and switches to ensure proper physical connection.

6.16.2 STM FC Failure to OASyS (Modbus Interface) – Total Loss of Interface (1,4)

6.16.2.1 Failed Component and Description of Failure

Modbus communications failure between the FC and SCADA host.

6.16.2.2 Impact on Operations / System and Severity

Database configuration ensures the communications path between the FC and the SCADA host are monitored. TPL has redundancy built-in to ensure constant monitoring of Modbus data unless complete site/station or system failure occurs.

The FC will monitor all deliveries even if no communications to the Host.

- If the loss occurred before the delivery started, then a new batch_id will be downloaded when communications return.
- If the whole delivery was offline a new batch id will be generated on upload.
- Transient communications loss will have no impact on the delivery other than the Batch Limits will not be generated on the Host.


If the delivery was performed offline, then the completed ticket will not have a Source and Destination field completed.

When communications are lost between FC and SCADA, the product type is set to "UNKNOWN-PRODUCT" and the comment field is set to "COMMS-LOSS" in the pending ticket. Where you see these updates depends on the state of the ticket prior to comms loss and the state upon recovery of comms loss.

If there is an active ticket running and communication recovers with the same active ticket, the active ticket will not be affected. The updates would be only within the pending ticket.

If there is an active ticket running and communications recovers with a different active FC ticket, the pending ticket will advance, and you will see the "UNKNOWN-PRODUCT" and "COMMS-LOSS" in the current active ticket.

If there is an active ticket running and communication recovers with the no active ticket, the updates would be only within the pending ticket.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 59 of 68

If there is no active ticket running and communication recovers with an active FC ticket, the pending ticket will advance and you will see the "UNKNOWN-PRODUCT" and "COMMS-LOSS" in the active ticket.

If there is no active ticket running and communication recovers with a no active FC ticket, the updates would be only within the pending ticket.

6.16.2.3 Typical Cause of Failure

- Loss of rack power; or
- Network outage/failure

6.16.2.4 Means of Detection and Controls

SCADA host will provide error logs and events that indicate Modbus failure between FC and SCADA host. Alarms for communications failures with the FC will provide an indication to the operator.

An alarm will be given to the operator on the loss of Communications to the FC.

6.16.2.5 Rectification and Impact of Rectification

Check firewall settings, routers, and switches for this connection.

Check database point configurations for related remote and connection records to ensure that IP addresses and ports are correct for the specified protocol.

6.16.2.6 Preventative Maintenance

Check wiring and cables between routers and switches to ensure proper physical connection.

6.16.3 Host Failure which communicates to the STM\PRV FC (1,2,6)

Failure is as per Section 6.7 as OASyS sees the FCs like a normal remote. Communication can be done from the Station or the MCC.

Note the fallback to the MCC polling for metering is complex for the following reasons,

- The batch id number generation is done on a site. The MCC is seen as another site and will thus if used, have a different number range.
- The PLC and Metering work together and as such both should be swung over together.

As a consequence of this complexity, metering will not be used whilst in the fallback position.

Note that under normal circumstances, metering can be executed from the MCC as long as the host server is on-site.


6.16.4 FC Failure to OASyS (Web Services Interface) (2,4)

6.16.4.1 Failed Component and Description of Failure

Web Services communications failure between the FC and SCADA host.

6.16.4.2 Impact on Operations / System and Severity

The reports will not be available in the reporting platform. For completed tickets, the FC docket information will not be uploaded, and will not be replicated to the SAP Landing table in the DSS.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 60 of 68

Reports are uploaded from Stream FC using Web Services interface and these reports need to be stored for processing. The FC has limited space to store reports and contain circular buffer where old reports are overwritten, and this may result in loss of information if these reports are not uploaded to the SCADA host before the reports are cycled.

FC Reports (incl. Consignee Batch, Hourly and Daily reports) will be able to be printed directly from the respective FCs, provided they are available on the FCs. These printed reports may be issued to SAP for processing if they have expired in the FC and cannot be uploaded.

6.16.4.3 Typical Cause of Failure

- Loss of rack power;
- FC failure/malfunction
- Network outage/failure

6.16.4.4 Means of Detection and Controls

SCADA host will provide error logs and events that indicate Web Services failure between FC and SCADA host. Alarms for communications failures with the FC will provide an indication to the operator.

6.16.4.5 Rectification and Impact of Rectification

Check switches for this connection.

Check database point configurations for related remote and connection records to ensure that IP addresses and ports are correct for the specified protocol.

6.16.4.6 Preventative Maintenance

Check wiring and cables between flow computers and switches to ensure proper physical connection.

6.16.5 Malformed Report (Web Services Interface) (2)

6.16.5.1 Failed Component and Description of Failure

The FC creates a report with characters of formats which are unexpected by the Host.

6.16.5.2 Impact on Operations / System and Severity

The reports will not be available in the reporting platform. For the completed tickets, the ticket information will be missing, and will not be replicated to the SAP Landing table in the DSS.


FC Reports (incl. Consignee Batch, Hourly and Daily reports) will be able to be printed directly from the respective FCs, provided they are available on the FCs.

6.16.5.3 Typical Cause of Failure

- Incorrect upload file;
- FC config change;
- An unexpected value in the report.

6.16.5.4 Means of Detection and Controls

SCADA host will provide error logs and events that indicate Web Services failure between FC and SCADA host. Alarms for failures with the FC will provide an indication to the operator.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 61 of 68

6.16.5.5 Rectification and Impact of Rectification

Investigate what caused the error via the logs and rectify. A log file exists on the upload host which will detail the causes of an upload error.

6.16.5.6 Preventative Maintenance

None.

6.16.6 STM FC Failure to PRV FC (3)

6.16.6.1 Failed Component and Description of Failure

The link between the Stream FC and the Prover FC fails (RS422) either through card failure or cable failure.

6.16.6.2 Impact on Operations / System and Severity

Proving will not be available from the Host.

6.16.6.3 Typical Cause of Failure

- Stream\Prover FC;
- Cable Failure.

6.16.6.4 Means of Detection and Controls


SCADA host repeats the FC alarms to the system, so the standard PRV communication failure alarm will be generated.

6.16.6.5 Rectification and Impact of Rectification

Check FC cards and communications cable.

6.16.6.6 Preventative Maintenance

None.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 62 of 68

6.17 Failure of Reporting Server

6.17.1 Failed Component and Description of Failure

Reporting Services for TPL is installed on a RealTime server. Where there is redundancy of RealTime services such as on Metering sites and the MCC, it is only installed on the RealTime side A server.

On metering sites and the MCC, a second Virtual Machine is created such if the main reporting instance fails, a second instance can be started up.

6.17.2 Impact on Operations / System and Severity

When the Reporting Server fails on the RealTime Server of a station, this associated Windows service will not be running. Since the stations replicate data to the MCC, these reports from the stations will be available at the MCC.

When MCC or DSS Reporting Server fails, the local stations will contain the data and the reports, and when the MCC and DSS Reporting Server recovers, the local stations will replicate data to allow for MCC and DSS to generate the needed reports.

6.17.3 Typical Cause of Failure

- Virtual Machine failure; or
- Loss of rack power; or
- Network outage/failure.

6.17.4 Means of Detection and Controls


If Reporting Server fails, Windows logs will show failure.

Client applications, such as displays running from XOS stations will not be able to obtain requested reports.

6.17.5 Rectification and Impact of Rectification

Restart of Reporting service and if that does not recover, then restart of the RealTime server in accordance to the SCADA host recovery procedures.

Switch over to the backup server is manual and done on the Diagnostics page as shown below:

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 63 of 68

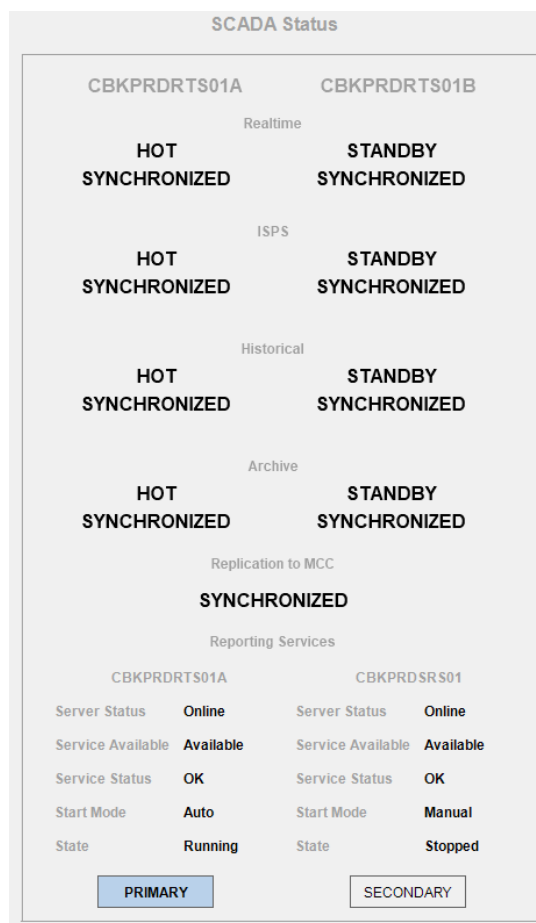



Figure 2: Reporting Fail-Over

For single server stations, if a manual SSRS failover was done the system will automatically point to the new reporting source (e.g. MCCPRDSRS01).

6.17.6 Preventative Maintenance

Review performance monitor reports and check logs on the server to ensure memory usage and disk space is available.

Ensure workstation has the latest operating system updates.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 64 of 68

6.18 Islanded Operations

The Station SCADA systems infrastructure allows for long network outage Islanded operations. The Station SCADA infrastructure includes:

- Station SCADA server(s), including RealTime and Historical operation, with complete functionality to manage the station. Redundant Station SCADA servers are provisioned at the stations that are normally manned (e.g. Coalbrook) and non-redundant servers are proposed for the other stations. A standby server can be added at any time in the future to make a redundant pair.
- Station HMI, which can connect to the Stations SCADA or to the MCC. In normal operation, the HMI is connected to the Station SCADA servers;
- Domain Controller, to securely manage access to the system. The Station Domain Controllers automatically synchronize with the Primary Domain Controller at the MCC and in Islanded Operations can operate autonomously; and
- Station Extended Editor (XE) application. The OASyS XE applications allow authorized users to make modifications to the Station SCADA database, displays, and configuration.

In the Islanded mode, the Station SCADA System continues to provide all SCADA operational and administrative functionality.


Upon reconnection with the MCC:

- The Domain Controller synchronizes with the DC at the MCC and any changes done in the authentication profiles will be consolidated through the system;
- The changes done at the Station SCADA displays must be manually copied to the Engineering system at the MCC;
- The RealTime and Historical data at the Station SCADA will be replicated with the MCC and in turn the MCCDSS.

OASyS DNA operates on a robust network model that includes redundancy and enhanced security. To facilitate support and administration, the network model is designed to be self-healing, with critical functions and devices supervised by health-monitoring software. In the event that a critical component fails, the system readjusts the data path to ensure that critical processes remain accessible to operators.

The Local Area Network (LAN) configuration is offered through a single “virtual” concept that provides the reliability of a dual-LAN network with the ease of use of a single-LAN network. TPL will find this system network yields increased uptime and better connectivity for both AVEVA-sourced and third-party applications. OASyS DNA’s standard architecture applies a fully-integrated network encryption utility to ensure the data interfaces between the Production SCADA system and the DSS is secured.


Reliability is backed by the partnering of responsibilities so that if a single component fails, its partner automatically takes over without impacting critical components of the system. OASyS DNA is structured with flexibility so that TPL can utilize multiple control sites as needed in a distributed environment. OASyS DNA can be scaled to suit the exact redundancy requirements of TPL.

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 65 of 68


7 APPENDIX A – REALTIME PROCESSES

TPL list of RealTime processes

Process Name	Critical Process	Description
ACEEngine	False	ACE Engine process
AgeWatchdog	True	Age Watchdog for monitoring telemetered points to ensure that they are actively being krunched
AlarmInterface	True	TPL specific application to interface with SCADA alarming by providing feedback on flow computer alarms
AlarmSerialization	True	SCADA alarm service that serializes alarms from all realtime processes
AORLegacyPubSubClientSupport	False	Legacy support for PubSubClient where AORs were once managed in RTDB (realtime database)
AORLegacySync	True	Legacy support for AORs which were once managed in RTDB (realtime database) to synchronize with AD LDS
arbMonitor	True	A part of the core OASyS arbitration process responsible for monitoring and synchronizing SCADA services to ensure always a hot service available
arbRx	True	A part of the core OASyS arbitration process responsible for receiving messages and updating the state of the service running on the other host
arbTx	True	A part of the core OASyS arbitration process responsible for opening a TCP/IP socket and transmitting messages containing the state of the service on the current host
BLTHostAce	True	BLT process used for ACE (Advance Calculation Engine)
BLTHost_LMS	True	BLT process used for LMS (Liquids Management Suite)
BLTHost.OPCProto	True	BLT process used for OPC protocol
BLTHost.RealTime	True	BLT process used for RealTime
BLTHost.RealtimeOGP	True	BLT process used for Realtime Oil and Gas Platform
BLTHost.RealtimeTPL	True	BLT process used for RealTime custom TPL
BLTHost.RVE	True	BLT process used for RVE (Rules Validation Engine)
BLTHost.UPM	True	BLT process used for UPM (Unit Power Management)
cbkCMXRELOCAL	True	Replication process for system CBK
checkCover	True	Process to check non-covered alarms


TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 66 of 68

CMXPersistenceStore	True	Process that fulfils integrity update requests for Publish/Subscribe topics in RTDB to clients such as XOS to subscribe to topics of interest
collect	True	Process checks at each cycle to determine if there is a point in the database that needs to be sampled
connectioncontroller	True	Process to monitor connections for available lower cost connections to use
dnaHealthMonitor	True	A part of the core OASyS process to handle critical problems of a service by providing indicators and performing failovers if necessary. Each OASyS service starts an instance of the dnaHealthMonitor where the instance is monitored within the dnaHealthMonitor process.
dnaService.REALTIME	True	A part of the core OASyS startup process to initiate arbitration and health monitor services.
FlowbossDownload	True	TPL process to download FloBoss flow computer reports
FlowComputerProcessor	True	TPL process to manage, monitor, and synchronize with control flow computer data
JSH	True	Job Scheduler process for periodic scheduled execution of system or user defined functions
logAdminPages	True	Process that writes adminPages to OASyS alarm and event specific mechanisms
ManualOverrideAlarm	True	Perform manual overrides on select RealTime records
monitorBatchTransfer	True	LMS process for control and monitoring of batch information
monitorBatmtr	True	Legacy LMS process for control and monitoring of batch information as well as metering data
monitorDOASConfig	True	Process that keeps the RealTime distribusys and privilege data synchronized with Historical
monitorLMSObjects	True	Liquid functionality to perform periodic operations to pump table
monitorSuppression	False	Process that monitors and controls select RTDB groups for alarm suppression
OMNICOMM MainOmni	True	OASyS SCADA communications process to control and manage the transfer of data between RTDB and remote devices
pressmon	True	LMS process to monitor pressures within a pipeline
ProcessMonitor	True	Allows applications to be started within this process so that they can be monitored for processing time and any critical failures requiring a failover

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 67 of 68

prodmove	True	Process for control, monitor, and management of products within a pipeline
productMonitor	True	LMS process that monitors product changes within a pipeline
ProverManager	True	TPL process to control, monitor, and manage prover flow computers
QueueHealthMonitor	True	Process that monitors the health of RealTime data queues
RealTimePerfMon	False	Process that calculates RealTime database statistics
remote_sched	True	Process that runs at the top of the minute and runs remote database scheduled commands
SecondTimer	True	Time-out handler process
TelemeteredTblMonitor	True	Performs periodic processing on select RealTime tables
TIMER	True	Process counts down all of the active timers and automatically calls the specified time-out handlers when a timer expires
unlock	True	Process to release locks held by dead processes
VirtualFlowComputer	True	OASyS host process that validates and corrects meter data
XACTCommandQSpooler	True	Process to redirect and persist messages to the historical database

Table 7.1

TRANSNET PIPELINES			
Document Name	Document Number	Revision Number	Page
SCADA System Architecture Failure and Recovery Mode Analysis	PRJ: E354086-00000-271-078-0013 TPL: TPL-XXXX-X-X-XXXX-XXXX	03 XX	Page 68 of 68