ESKOM
RESEARCH, TESTING AND DEVELOPMENT

TECHNICAL REPORT FOR RESEARCH

CONFIDENTIAL

REPORT TITLE	:	**RFI SPECIFICATION (LEGACY TO IP MIGRATION)**

REPORT REF No	:	RES/SR/21/1962996
PROJECT NAME	:	Legacy Interfaces/Protocols to IP Migration
PROJECT No	:	N.RA50015
STEERING COMMITTEE	:	Tx Plant Performance and Asset Managemnet
AUTHORS	:	Joel Mataboge
DEPARTMENT	:	Tx Asset Management

TECHNICAL REPORT FOR RESEARCH

RFI SPECIFICATION (LEGACY TO IP MIGRATION)

REPORT REFERENCE NO:	RES/SR/21/1962996		
DATE:	10 FEBRUARY 2022		
COMPILED BY:	JOEL MATABOGE	SIGNED	10/02/2022 DATE
ACCEPTED BY:	ZWELANDILE MBEBE	SIGNED	14/02/2022 DATE
AUTHORISED BY:	DR. PRATHABAN MOODLEY	SIGNED	17.02.2022 DATE

CONTENTS **PAGE**

EXECUTIVE SUMMARY

RFI SPECIFICATION (LEGACY TO IP MIGRATION)

BACKGROUND

- Most of the Eskom Operational Technology (OT) end devices connect on the Eskom Telecommunications network using legacy interfaces and protocols. One of the long-term network replacement objectives is to replace the Bandwidth Management Equipment (BME) network with Internet Protocol / Multi-Protocol Label Switching (IP/MPLS). This means all legacy interfaces and protocols must be catered for in the IP/MPLS solution and this escalates the network replacement costs while also resulting in complex IP network designs and operations.
- As a measure to curb complex networks designs/operations and escalated replacement cost a decision was taken to research if it is possible to migrate legacy interfaces/protocols to IP. Representatives from different line groups were consulted and they gave input on their readiness to migrate to an IP platform. A working group named Legacy to IP Workgroup was established, in which all the stakeholders formed part of. The purpose of the working group was to identify initiatives, which will facilitate and accelerate the migration of end devices from legacy interfaces and protocols to IP. The working group was tasked with the following:
  - Assess the existing legacy requirements
  - Identify opportunities where end user equipment can migrate from legacy interfaces and protocols to IP.
  - Produce a report, which must be signed by the end users.
  - Initiate necessary pilots for testing any of the proposed migration plans with the relevant study committee/ end users.
  - The working group carried out the tasks above from which opportunities were identified to migrate IP ready end devices from legacy interfaces and protocols to IP. It was identified that there is still a lot of equipment which is not IP ready and the report proposed that a market research shall be done to establish if there are IP replacement devices. These devices shall connect to an IP/MPLS network using IP interfaces and protocols and render the equivalent or better performance as their legacy counterparts.

DESIGN OBJECTIVES AND ASSUMPTIONS

The objective of this exercise is to interrogate the market and establish if it is possible to eliminate all legacy interface/protocols on the proposed packet switched network. This can be done by first determining if there are subcomponents (i.e. IED cards that have IP interfaces), that can replace the legacy subcomponents on the existing OT end user devices, front end systems and associated protocols. In an event where the IP components for migrating the existing sytems are non-existent in Eskom, research must be carried out in order to determine if IP equivalent devices to the legacy devices exist. Once all has been established, these devices must be piloted on an IP/MPLS network.

METHODOLOGY

In order to satisfy the objective of this research, a quantitative research will be held. Quantitative research is defined as social research that employs empirical methods and empirical statements. An empirical statement is defined as a descriptive statement about what “is” the case in the “real world” rather than what “ought” to be the case. Typically, empirical statements are expressed in numerical terms. Another factor in quantitative research is that empirical evaluations are applied. Empirical evaluations are defined as a form that seeks to determine the degree to which a specific program or policy empirically fulfils or does not fulfil a particular standard or norm. An RFI will be designed and disturbed to various relevant institutions and organisations, to determine the maturity, adoption and operation of IP end-devices interfaces/protocols in an OT environment.

RESULTS / FINDINGS

From the concept phase, it was discovered that there is a significant installed base of applications/services that are based on legacy interfaces. Of these end devices, some of them are used to implement mission critical services such as teleprotection and tele-control. This implies that care must be taken when migrating these services to IP. Although literature study reveals that there are standards that ensure smooth operation of these services on an IP environment, care must be taken when migrating from serial to internet protocols. The following serial communications interfaces and electrical interfaces within Eskom were identified:

- X21
- X25
- RS232
- RS422/RS485
- E&M
- FXO/FXS
- IEC 101
- DNP3
- Dial up moderms

RECOMMENDATIONS

Below are the recommendations from the scan report:

- An RFI to be issued, to determine maturity and industry support for IP based OT applications.
- Suppliers to demonstrate functionality of their applications, this will give Eskom an opportunity to determine whether their requirements will be fulfilled going forward.
- Suppliers to recommend standards and protocols for IP based OT applications, and their compliancy thereof.
- Suppliers are also encouraged to present peripherals (cards) that are IP based, since there is a significant installed base of legacy devices, procuring IP modules will make sense as compared to replacing the whole unit.

- A roadmap, and strategies on how the migration will be implemented must be prepared, or revised (if they exist), this will ensure seamless transition.

CONCLUSIONS

The RFI will fast track the process of identifying cost effective and simple techniques of accomodating legacy devices on packet networks.

KEYWORDS

Internet Protocol, Legacy, teleprotection, cybersecurity, latency, encyption/decrption

ITEM DETAILS

Steering Committee	:	Tx Plant Performance and Asset Managemnet
Report Number	:	RES/SR/21/1962996
Project No	:	N.RA50015
Project Name	:	Legacy Interfaces/Protocols to IP Migration
Project Manager	:	JOEL MATABOGE
Contact Number	:	072 632 0849
Customer	:	Nelson Luthuli
Financials		
Actual Cost of this Task	:	R 330k
Cost to Implement	:	R 100m

RETURN ON INVESTMENT

It must be noted that the values used here are estimated. Assuming that this RoI is calculated over 5 years:

- Estimated value of refurbishing end user devices: R100m
- Estimated savings on maintenance: R50m per annum
- Estimated savings on retaining legacy skills: R30m per annum
- Estimated savings on provisioning: R5m per annum
- Total estimated savings over 5 years R4m

$$RoI = \frac{Gain\ from\ Investment - Cost\ of\ Investement}{Cost\ of\ Investment}$$

$$RoI = \frac{R425m - R100m}{R100m}$$

$$RoI = 3.25$$

ABBREVIATIONS LIST:

Abbreviation	Description
DFR	Digital Fault Recorders
DNP	Distributed Network Protocol
EMC	Electromagnetic Compatability
EMI	Electromagnetic Interference
EPU	Electric Power Utility
ET	Eskom Telecommunications
FEP	Front End Process
GPS	Global Positioning System
IEC	International Electrotechnical Commisison
IED	Intelligent Electronic Devices
IP	Internet Protocol
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching
MS	Master Station
OEM	Original Equipment Manufacturer
OT	Operational Technology
PoC	Proof of Concept
QoS	Quality of Supply / Quality of Service
RFI	Request for Information
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TDM	Time Division Multiplexing
TPE	Teleprotection Equipment
TWS	Travelling Wave Systems
UHF	Utra High Frequencies
VHF	Very High Frequrencies
WAN	Wide Area Network

LIST OF TABLES

RFI SPECIFICATION (LEGACY TO IP MIGRATION)

1 INTRODUCTION

Eskom Holdings Limited ("Eskom") invites you to submit information on cost effective and simplified integration of legacy Electric Power Utility (EPU) Intelligent Electronic Device (IEDs) and associated front end systems on the IP/MPLS network. Currently, Eskom's install base consists of a number of legacy IEDs which connect to the Eskom telecommunications Time Division Multiplexing (TDM) network and front end OT systems using legacy interfaces/protocols. These legacy systems offer reliable services due to the deterministic nature of TDM networks. Eskom intends on migrating its network to a packet based network (IP/MPLS). Carrying of legacy IEDs on this packet network will inevitably introduces complex designs and additional costs associated with legacy interfaces.

Packet technologies are adopted in OT (Operational Technology) environments and are expected to offer TDM like or even better performance and must support the stringent OT communication requirements. This has prompted Eskom to conduct research on cost effective and simplified integration of legacy IEDs and front-end systems to IP/MPLS network. Where it is not possible to find cost effective and simplified means of integrating any of the existing legacy IEDs and front-end systems to the packet network, suppliers are requested to provide information on alternative solutions.

Suppliers must indicate if they are willing to provide the proposed integration equipment and alternative solutions for testing at their own cost. Suppliers shall provide sample reports from their client's live installations, demonstrating performance of the proposed solution. Where such systems are still being tested in the lab, the supplier shall clearly state that the results are for lab based installations.

2 RFI SCOPE

The scope of this Request for Information (RFI) includes IEDs and front end system for the following services:

- Tele-protection
- Supervisory Control and Data Acquisition (SCADA)
- Quality of Supply (QoS) and metering
- Digital Fault Recorder (DFR)
- Travelling Wave Systems (TWS)
- Analogue UHF and VHF radios for voice and SCADA

Suppliers are requested to provide information on the most cost effective means for connection of the existing Eskom legacy IEDs and Front end systems to the IP/MPLS network. Choice of protocols, interfaces, and used converters must be stated. The following are the installed devices in Eskom:

Table 1: ET (Eskom Telecommunications) services with legacy interfaces/protocols

Service		Devices	Physical Interfaces and Protocols
Tele-protection		NSD570, DIP5000	X21,E1
Telecontrol/SCADA		Talus RTU, GE D400, ABB RTU 560, GE D20, COM 300	RS232, RS232/422 Converter, RS485/RS422(4w), IEC60970-5-101, DNP
QoS and metering		ION 8800,	RS232, RS485, , Mobile Protocols (GMS, GPRS, UMTS, HSDPA, etc.)
DFR		P531	X.25(RS232)
TWS		Hathaway Telefault TWS MK2 or MK3	56 k Dial-up modem
Analogue UHF radios (SCADA)		TB 8100	RS232
Analogue VHF radio (Voice)		TB 8100	E&M

3 REQUIREMENTS

Taking into consideration the above services, Eskom requires potential suppliers of OT (Operational Technology) to provide information and a presentation on the strengths, weaknesses and roadmap of related technologies as it applies to a utility environment.
The information and presentation must include but not be limited to the requirements listed below:

3.1 TELE-PROTECTION

Eskom employs Tele-protection Equipment (TPE) that employs legacy interfaces (E1 support but mostly X.21 installed base). Eskom is investigating alternative interfaces and protocols which can natively connect on the IP/MPLS (network to reduce network costs and configuration complexity. It must be emphasized that the IPbased TPEs must be compliant with the stringent teleprotection requirements. This RFI seeks to determine if there exist TPEs that fully natively support IP interfaces/protocols, or if there exist peripherals and card or converters, that will eliminate the need of accommodating legacy interfaces and protocols on the IP/MPLS network. As a minimum, the provided information shall answer the following questions:

3.1.1 Which IP protocols are used for Teleprotection applications?
3.1.2 How many utilities are using IP protocols for Teleprotection applications and what is their experience thereof?
3.1.3 What are recommended telecommunication architectures when implementing IP protocols for Teleprotection applications?
3.1.4 What are the physical interfaces used for the Teleprotection applications?

3.1.5 Is the equipment compatible with substation EMC/EMI hardening standards, and what standards are those?

3.1.6 The supplier to provide performance information on actual installations of TPEs (Teleprotection Equipment Equipment) using IP interfaces in the power network.

3.1.7 What are other cost effective mechanisms that can be used to integrate serial interface based Teleprotection into a packet based communications network (backbone)?

3.1.8 Is the a cost effective, scalable converters based to integrate the as is legacy teleprotection solution to IP/MPLS?

3.1.9 What is the performance and cyber security impact of using a converters based solution?

3.1.10 What form of cyber security management is used?

3.1.11 Is the cyber security implemented on the WAN/LAN or the end device(s)?

3.1.12 What architecture(s) is used to enable cyber security?

3.1.13 Is all Teleprotection traffic encrypted, and what encryption mechanism is used?

3.1.14 What effect does encryption and cyber security have on the performance of the Teleprotection applications?

3.2 TELECONTROL/ SCADA

Eskom Supervisory Control and Data Acquisition (SCADA) system is currently based on IEC 60870-5-101 in Transmission and DNP3 in Distribution. Front end and RTU interfaces are based on legacy serial interfaces including RS232, RS485 and X.21 asynchronous/RS422 interface. Supplies are required to propose alternative IP based SCADA system with protocols and interfaces which natively connect as IP on Eskom IP/MPLS network. End-to-end packet based solution will simplify the design significantly and ensure the organisation is ready for dicontinuation of legacy technologies. As minimum, the provided information shall answer the following questions:

3.2.1 Which IP protocols are used for Telecontrol/SCADA applications?

3.2.2 How many utilities are using IP protocols for Telecontrol/SCADA applications and what is their experience thereof?

3.2.3 What are recommended architectures when implementing IP protocols Telecontrol/SCADA applications?

3.2.4 What are physical interfaces used for the Telecontrol/SCADA applications?

3.2.5 Is the equipment compatible with EMC/EMI hardening substations standards, and what standards are those?

3.2.6 How complete is the IEC61850 standard for inter-substation communication.

3.2.7 What are performance requirements for IEC61850 for inter-substation communication?

3.2.8 Provide readiness of utilities to meet performance requirements specified in 3.2.7 above.

3.2.9 Is there a need to use different protocols for Distribution and Transmission SCADA applications?

3.2.10 How do we migrate from IEC60870-5-101 to IP based protocols e.g. IEC61850, DNPoIP, and IEC60870-5-104?

3.2.11 Provide OEM roadmaps for energy management systems with regards to packet based protocols for Telecontrol/SCADA applications?
3.2.12 Can IEC60870-5-104 handle message sequencing?
3.2.13 What is the impact of migration to IP on the lifecycle of all involved equipment?
3.2.14 What are available transitioning options in the migration process taking into account the installed base?
3.2.15 How do we make sure that the Proof of Concept (PoC) does not work only in the PoC environment but fail in the other installation scenarios?
3.2.16 Provide uses case for unique SCADA services characteristics/ configurations?
3.2.17 How do you make sure that the systems does not work well initially and then fail a few years down the line?
3.2.18 What is the alternative solution to GPS time stamping? There no are GPSs in most of the sites.
3.2.19 How is performance on the SCADA system measured?
3.2.20 What are software requirements of the SCADA MS?
3.2.21 Is there a cost effective, scalable converters based solution to integrate the as is legacy SCADA solution to IP/MPLS?
3.2.22 What is the perfomance and cyber security impact of using a converters based solution?
3.2.23 What are future trends for substation architectures and equipment technologies whilst using IP protocols for front end and RTU interfaces?
3.2.24 What form of cyber security management is used?
3.2.25 Is the cyber security implemented on the WAN/LAN or the end device?
3.2.26 What archirctrure(s) is used to enable cyber security?
3.2.27 Is all SCADA traffic encrypted, and what encryption mechanism is used?
3.2.28 What effect does encryption and cyber security have on the performance of SCADA?
3.2.29 What are cybersecurity considerations in implementing IEC61850 for inter-substation communications
3.2.30 What are cybersecurity considerations in migration of SCADA from serial to IP based systems (End-to end).
3.2.31 Detail the foreseeable cyber security exposure and mitigations.
3.2.32 What is the impact of cybersecurity implementation on latencies?
3.2.33 How far is the IEC 62351 (Security Mechanism for IEC61850 Message Exchanges) standard and what can be extracted from this standard to support this initiative?
3.2.34 Is it possible to introduce authentication between RTU and the FEP without introducing latencies?
3.2.35 How can we reduce costs for the firewalls required in each substation?

3.3 QOS AND METERING

3.3.1 Which IP protocols are used for QOS and metering applications?
3.3.2 How many utilities are using IP protocols for QOS and metering applications and what is their experience thereof?
3.3.3 What are recommended architectures in implementing QOS and metering based on IP protocols?
3.3.4 What are physical interfaces used?

3.3.5 Is the equipment compatible with substation EMC/EMI hardening standards, and what standards are those?

3.3.6 Is there a cost effective, scalable converters based solution to integrate the as is legacy metering solution to IP/MPLS?

3.3.7 What is the perfomance and cyber security impact of using a converters based solution

3.3.8 What form of cyber security management is used?

3.3.9 Is the cyber security implemented on the WAN/LAN or the end device?

3.3.10 What archircture(s) is used to enable cyber security?

3.3.11 Is all QOS and metering traffic encrypted, and what encryption mechanism is used?

3.3.12 What effect does encryption and cyber security have on the performance of the QOS and metering applications?

3.4 DIGITAL FAULT RECORDERS

3.4.1 Which IP protocols are used for DFR applications?

3.4.2 How many utilities are using IP protocols for DFR applications and what is their experience thereof?

3.4.3 What are recommended architectures in implementing DFR based on IP protocols?

3.4.4 What are physical interfaces used?

3.4.5 Is the equipment compatible with substation EMC/EMI hardening standards, and what standards are those?

3.4.6 Is there a cost effective, scalable converters based solution to integrate the as is legacy DFR solution to IP/MPLS?

3.4.7 What is the performance and cyber security impact of using a converters based solution?

3.4.8 What form of cyber security management is used?

3.4.9 Is the cyber security implemented on the WAN/LAN or the end device?

3.4.10 What archircture(s) is used to enable cyber security?

3.4.11 Is all DFR traffic encrypted, and what encryption mechanism is used?

3.4.12 What effect does encryption and cyber security have on the performance of the DFR applications?

3.5 TRAVELLING WAVE SYSTEMS (TWS)

3.5.1 Which IP protocols are used for TWS applications?

3.5.2 How many utilities are using IP protocols for TWS applications and what is their experience thereof?

3.5.3 What are recommended architectures in implementing TWS based on IP protocols?

3.5.4 Is the equipment compatible with substation EMC/EMI hardening standards, and what standards are those?

3.5.5 Is there a cost effective, scalable converters based solution to integrate the as is legacy TWS solution to IP/MPLS?

3.5.6 What is the performance and cyber security impact of using a converters based solution?

3.5.7 What are physical interfaces used?

3.5.8 What form of cyber security management is used?

3.5.9 Is the cyber security implemented on the WAN/LAN or the end device?

3.5.10 What archircture(s) is used to enable cyber security?
3.5.11 Is all TWS traffic encrypted, and what encryption mechanism is used?
3.5.12 What effect does encryption and cyber security have on the performance of the TWS applications?

3.6 ANALOGUE UHF (SCADA)

3.6.1 Which IP protocols are used for analogue UHF applications?
3.6.2 How many utilities are using IP protocols for analogue UHF applications and what is their experience thereof?
3.6.3 What are recommended architectures in implementing analogue UHF based on IP protocols?
3.6.4 What are physical interfaces used?
3.6.5 Is the equipment compatible with substation EMC/EMI hardening standards, and what standards are those?
3.6.6 Is there a cost effective, scalable converters based solution to integrate the as is legacy UHF solution to IP/MPLS?
3.6.7 What is the performance and cyber security impact of using a converters based solution?
3.6.8 What form of cyber security management is used?
3.6.9 Is the cyber security implemented on the WAN/LAN or the end device?
3.6.10 What archircture(s) is used to enable cyber security?
3.6.11 Is all analogue UHF traffic encrypted, and what encryption mechanism is used?
3.6.12 What effect does encryption and cyber security have on the performance of the analogue UHF applications?

3.7 ANALOGUE VHF (VOICE)

3.7.1 Which IP protocols are used for analogue voice applications?
3.7.2 How many utilities are using IP protocols for analogue voice applications and what is their experience thereof?
3.7.3 What are recommended architectures in implementing analogue voice based on IP protocols?
3.7.4 What are physical interfaces used?
3.7.5 Is the equipment compatible with substation EMC/EMI hardening standards, and what standards are those?
3.7.6 Is there a cost effective, scalable converters based solution to integrate the as is legacy DFR solution to IP/MPLS?
3.7.7 What is the performance and cyber security impact of using a converters based solution?
3.7.8 What form of cyber security management is used?
3.7.9 Is the cyber security implemented on the WAN/LAN or the end device?
3.7.10 What archircture(s) is used to enable cyber security?
3.7.11 Is all analogue voice traffic encrypted, and what encryption mechanism is used?
3.7.12 What effect does encryption and cyber security have on the performance of the analogue voice applications?

4 ADDITIONAL INFORMATION

4.1 ROADMAP

At minimum, the supplier shall provide the following roadmap information:

4.1.1 Technology roadmap including the product datasheets.
4.1.2 Date of release for the proposed equipment: Describe the status of each release, for example as generally available, features to be released, features to be designed or by any equivalent terminology used by the vendor.
4.1.3 Planned upgrades for the next 5 - 10 years with the detailed planned changes on hardware and software.
4.1.4 Planned end of sale.

4.2 TECHNOLOGY SUPPORT IN SOUTH AFRICA

4.2.1 List the local and international suppliers for South Africa.
4.2.2 List the local and international support for South Africa.
4.2.3 List the number of local resources trained on the equipment with their levels of training.
4.2.4 Provide spare management philosophy/policy.
4.2.5 Provide manuals on equipment mentioned.
4.2.6 Support call centre capacity and fault logging options

4.3 TRAINING/SKILLS REQUIREMENTS IN TERMS OF COURSES AND DURATION OF TRAINING

4.3.1 Identify the training/skill requirements to install, operate and maintain the equipment.
4.3.2 Identify where training can be done for Eskom employees.

4.4 PERFORMANCE RESULTS ON COMPLETED AND EXISTING UTILITY DEPLOYMENTS INCLUDING REFERENCES

4.2.7 Please provide examples of previous projects and the results of these projects.
4.2.8 Provide a list of planned projects and estimated timelines.

5 CONCLUDING REMARKS

All hard copy documents provided must also be available as soft copies for evaluation.

Where presentations are required, Eskom may shortlist the number of presentation based on the following rules:

5.1 Comprehensiveness of submission directly addressing the information and presentation scope identified in this document. (supply of equipment brochures alone will not be adequate)

5.2 The most comprehensive submission will be invited.

The above shortlisting is only to allow for a manageable process and will not exclude any supplier to respond on future enquires.

Notwithstanding the above, Eskom reserves the right not to proceed with any further engagements on the technologies presented.

The invited participants agree that no discussion with Eskom or its employees or its agents in this context shall be construed to be an obligation to enter into any contract whatsoever, or commit Eskom in any way whatsoever.

6 DISTRIBUTION LIST

PROGRAMME MANAGER:	RONEL CLARKE
CUSTOMER:	NELSON LUTHULI
PROJECT OFFICE:	GILLIAN CRAWFORD (1 Bound & Hyperwave Link) PHUMIE TAKALANI (Hyperwave Link)
STEERING COMMITTEE:	TX PLANT PERFORMANCE AND ASSET MANAGEMNET
ADDITIONAL COPIES:	VOICE AND DATA CARE GROUP