COMMUNICATION SYSTEM FAILURE GUIDELINES

PREPARED BY:	National Connections
DOCUMENT REF:	NC-GDLN -0007
VERSION:	1
EFFECTIVE DATE:	18 December 2020
STATUS:	FINAL

Approved for distribution and use by:

APPROVED BY:	Mark Shilliday
TITLE:	Group Manager National Connections

DATE: 18 / 12 / 2020

PURPOSE

This document has been prepared by AEMO to provide guidance to Connection Applicants and Generators about AEMO's requirements around the design of communication systems installed within generating systems.

DISCLAIMER

This document may be subsequently updated or amended.

This document does not constitute legal or business advice, and should not be relied on as a substitute for obtaining detailed advice about the National Electricity Law, the National Electricity Rules, or any other applicable laws, procedures or policies. AEMO has made every effort to ensure the quality of the information in this document but cannot guarantee its accuracy or completeness.

Accordingly, to the maximum extent permitted by law, AEMO and its officers, employees and consultants involved in the preparation of this document:

- make no representation or warranty, express or implied, as to the currency, accuracy, reliability or completeness of the information in this document; and
- are not liable (whether by reason of negligence or otherwise) for any statements or representations in this document, or any omissions from it, or for any use or reliance on the information in it.

VERSION RELEASE HISTORY

Version	Effective Date	Summary of Changes
1.0	18 December 2020	First Issue

CONTENTS

TABLES

1. INTRODUCTION

1.1. Purpose and scope

This Guideline sets out AEMO's expectations for the operation of GSs following a communication failure in the one or more of the following main communication links within a GS:

- Primary PPC and Secondary PPC
- PPC and PPC meter
- PPC and GUs
- GUs and measurement unit
- PPC and *substation* equipment

This Guideline does not apply to any other type of communication system failure. The measures to be taken by a *Generator* following any other type of communication system failure must be approved by the NSP and AEMO.

1.2. Glossary

Terms defined in the NEL and the NER have the same meanings in this document unless otherwise specified. These terms are identified by italicising them, but failure to italicise a defined term does not affect its meaning.

The words, phrases and abbreviations in Table 1 have the meanings set out opposite them when used in this document.

Table 1 Defined Terms

Term	Meaning
Acknowledge	A SCADA function that is manually enabled by the Operator.
Category 1	Communication links between a GS' measurement units and controllers.
Category 2	Communication links between a GS' two or more controllers.
Changeover	The process by which a Secondary PPC takes over a GS' communication system following its Primary PPC's failure.
Communication Design Report	A document submitted with the R1 package as a *Generator*, describing a GS' communication system fail-safe mechanism.
ECM	*energy conversion model.*
FOBOT	Fibre optic break out tray.
GS	*generating system.*
GU	*generating unit.*
NEL	*National Electricity Law.*
NEM	*national electricity market.*
NER	*National Electricity Rules.*
NSP	*Network Service Provider.* Used in this Guideline to denote the *connecting Network Service Provider*.
NSP Operating Protocol	The operating protocol agreed between a *Generator* and an NSP with respect to how a particular GS will be operated by the Operator.
Operator	The physical operator of a GS, who could be the *Generator*, or someone authorised by the *Generator* to operate the *Generator's* GS.
PLC	Programmable logic controller.

PPC	Power plant controller.
Primary PPC	The main PPC used by a GS.
RTU	Remote terminal unit.
SCADA	Supervisory Control and Data Acquisition system.
Secondary PPC	The hot, standby, redundant PPC that takes over if a Primary PPC fails.
VCS	Voltage control strategy.
VDS	AEMO's Var Dispatch Scheduler.

1.3. Interpretation

The following principles of interpretation apply to this document unless otherwise expressly indicated:

(a) This Guideline is subject to the principles of interpretation set out in Schedule 2 of the NEL.

(b) Units of measurement are in accordance with the International System of Units.

2. RELATED AEMO DOCUMENTS

This document does not supersede or replace any other documents published by AEMO in accordance with the NER that relate its subject matter. Table 2 lists these and other related documents.

Table 2 Related AEMO Documents

Title	Location
R1 Submission Check List	
Power System Data Communication Standard	https://www.aemo.com.au/-/media/Files/Electricity/NEM/Network_Connections/Transmission-and-Distribution/AEMO-Standard-for-Power-System-Data-Communications.pdf

3. SUMMARY OF COMMUNICATION SYSTEM ARCHITECTURE

3.1. Communication System Hardware Definition and Limitations

A GS' communication system comprises the elements within the communication loop of the GS. The hardware platform is comprised of the physical components, including the meters, controllers, inverters (and its controllers), network switches, media and protocol converters, fibre and copper cables.

Hardware is vulnerable to failure due to electronic circuit failure, physical damage (common for cables), human error when replacing cables during maintenance, firmware crashes, stack overflow in Kernels, incompatible firmware updates, or the loss of *supply*.

3.2. Communication System Software and Firmware Definition and Limitations

All the controllers and network switches within the hardware of a GS's communication system must be equipped with firmware to execute a *control system's* algorithms and establish communication between different hardware within a GS. This communication involves encoding and decoding data packets.

For two pieces of equipment to communicate, they both have to "speak the same language" by using the same communication protocol. For instance, a measurement device needs to send information in a format that a controller will understand. If the two platforms do not use the same communication protocol, the GS' designer must add protocol converters or media converters into

the design. Adding protocol or media converters introduces a new point of failure and increases a signal's transmission time, known as the "signal time delay" or "signal transport delay". Depending on signal application, this can cause delays in the communication system, which can result in a breach of NER, a reduction in the stability margin of the GS' *control system* and, in extreme cases, unstable operation of the GS.

Software and firmware are susceptible to virtual issues, such as poor coding, incompatible firmware versions, incompatible communication protocols, poor communication system design coordination, poor communication network traffic and poor signal delay optimisation.

3.3. Categories of communication links

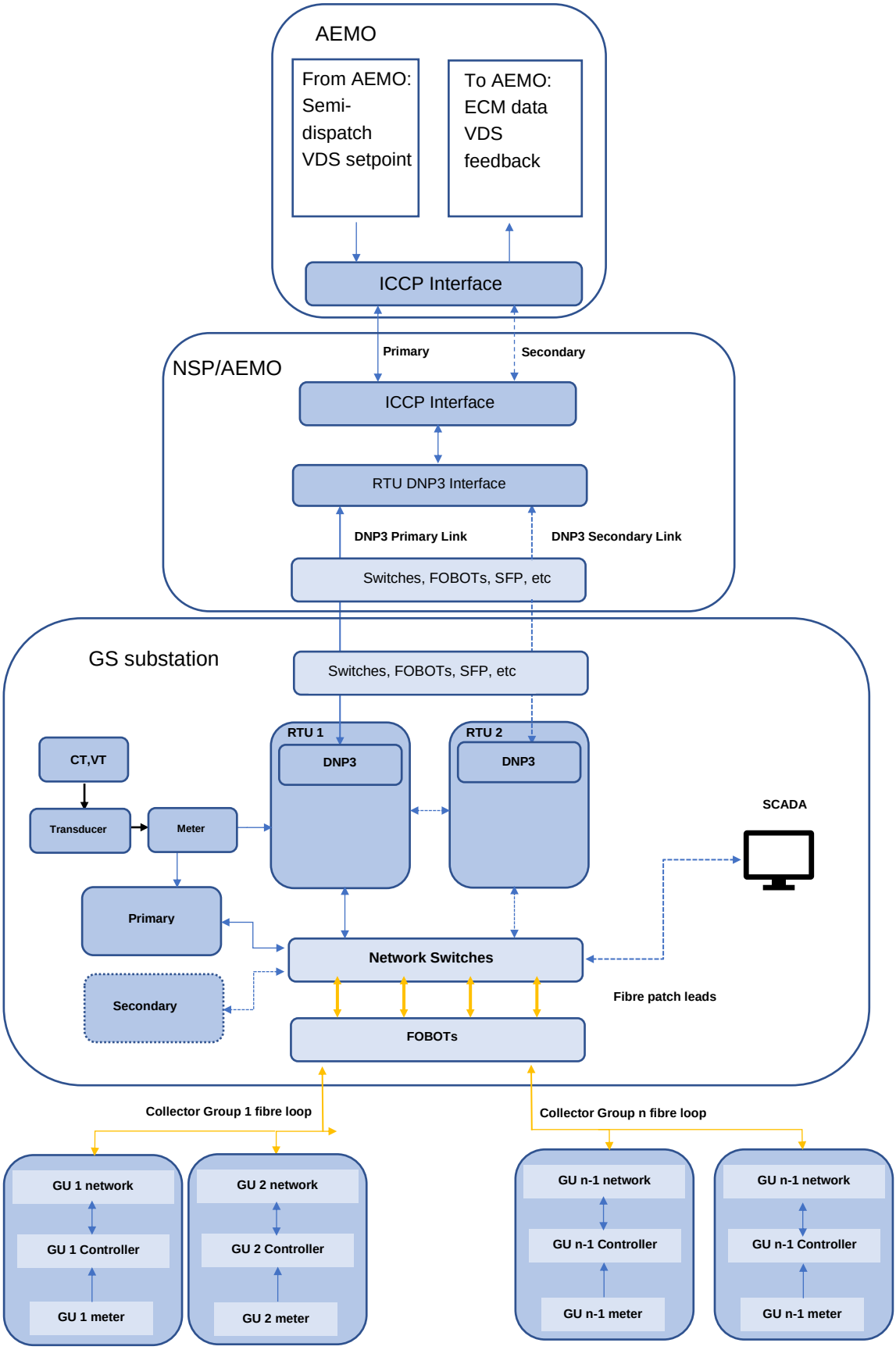
There are two types of communication links that are critical to a GS' design:

Category 1. These links send raw data from measurement devices to control and monitor certain aspects of a GS. The most notable examples include links between the *connection point meter* and the PPCs, and the communication link between the GUs and their measurement units (CT/VT or meter).

Category 2. These types of communication links connect the controllers for monitoring purposes and transferring setpoints only. Examples include a GS's SCADA to AEMO's SCADA via substation RTU-NSP's RTU, *substation* PLC/RTUs to PPCs, PPC to GUs.

Figure 1 illustrates a generic communication layout with the key devices and the communication links.

Figure 1. Generic Communication Topology



4. FAIL-SAFE COMMUNICATION DESIGN

Due to recent issues with the commissioning and operation of GSs in the NEM, AEMO considers that GS communication system failures pose a risk to *power system security*. As a result, AEMO requires all persons applying to register as a *Generator* to provide a Communication Design Report as part of its R1 package and ensure that its GS' communication system fail-safe mechanism operates as described in the Communication Design Report, which must be consistent with this Guideline. The Communication Design Report must detail all information required by this Guideline.

The Communication Design Report must detail all information specified by this Guideline.

4.1. Primary PPC and Secondary PPC, Communication and Control

Both Category 1 and Category 2 communication links can suffer link failures that can result in a breach of NER by disturbing a GS *control system's* measurements and setpoints.

4.1.1. Primary PPC failure where there is no Secondary PPC

PPC failure will not only stop the processing of PPC calculations, such as *connection point* calculations, but will also cause a communication failure with all measurement units and controllers that are directly or indirectly linked to the PPC. This can result in either or both of the following:

- All the measured quantities, such as the feedback of the control loops, are lost, do not update or are miscalculated.
- All PPC commands to external devices, including *substation* RTUs and the GUs, are lost, do not update or are miscalculated.

If *network* conditions change during a communication failure, this could result in the GS' responding to earlier *network* conditions, which could work against current *network* conditions, thereby exacerbating *network* issues, cause unstable GS operation or trigger the GS' or *network protection systems*.

To prevent these consequences:

1. GSs without a Secondary PPC must have a fail-safe mechanism, as described in this Guideline, that will operate in the event of PPC failure.
2. *Substation* controllers or SCADA must also detect a PPC failure within 5 sec and notify the Operator of the PPC failure by raising a latched fail-safe alarm.

Once the PPC failure is detected, the GS will go into non-generating mode, depending on the operational arrangement between the *Generator* and NSP (VCS or NSP Operating Protocol), auxiliary equipment, such as shunt reactive plant, active and passive harmonic filters, collector feeders and *transformers* may remain *connected* or *disconnected*.

4.1.2. Primary PPC failure where there is a Secondary PPC

Where a Secondary PPC is installed and the Primary PPC fails:

1. SCADA must detect the Primary PPC's failure within 5 sec through the fail-safe mechanism.
    a. One of the possible detection mechanisms is by monitoring Primary PPC communication.
    b. SCADA must raise an alarm that cannot self-reset.
    c. The Operator must communicate the Primary PPC failure to the NSP's and AEMO's *control rooms* in accordance with the NSP Operating Protocol.
2. The Changeover must be performed in no more than 500 ms.

3. The Changeover must be bumpless, with no change in the GS' *active power* and *reactive power* quantities.
    a. The Changeover must be observed as one PPC communication failure by its meters and the GUs lasting for only a few hundreds of milliseconds and recovering back to its previous status within that time.
    b. If the Secondary PPC requires a start-up, the Changeover delay and algorithm must have been approved by the NSP and AEMO as part of the GS' operational arrangement during the detailed design phase.
4. If the Primary PPC returns to a healthy operational status, the GS must not automatically revert to Primary PPC control without the Operator's knowledge.
    a. The process of reverting back to Primary PPC must only be done with the Acknowledgement of the Operator.
    b. Unless agreed otherwise between AEMO, the NSP and the *Generator*, the GS may revert to Primary PPC operation only when it is not generating *active power* and *reactive power*.

4.1.3. Secondary PPC Failure

The GS must follow the process described in section 4.1.1 if the Secondary PPC fails.

4.2. Communication Between PPC and PPC Meter

This communication link is a Category 1 and can be broken or disturbed due to: CT/VT to transducers wiring issue, transducer failure, transducer to meter wiring issue, meter firmware failure, disconnection of the communication cable between the meter and PPC, high volume of communication traffic between the PPC and the meter, or PPC communication firmware/driver failure.

The data flowing through this link includes the *connection point* power quantity measurements, which are used as feedback of the control loops, such as *voltage*, *frequency*, *active power* and *reactive power*. This feedback is critical in the control loops for preventing the GS from breaching the NER and causing unstable operation of the GS. Therefore, a GS' communication fail-safe mechanism must meet the following criteria:

1. The GS must detect the loss of communication (lack of update in *voltage*, *frequency*, *active power* or *reactive power* quantities) within 500 ms of the loss.
    (a) This may be done using a default Watchdog bit available within the communication protocol or by customised logic that continuously monitors communication with the GUs.
    (b) Note: Based on the GS models and commissioning data received by AEMO, AEMO considers that the outer closed-loop control of the *connection point* controllers should receive multiple samples of refreshed measurements as control feedback. The delay in receiving these packets of data decreases the stability margin of the GS' *control system* and, therefore, its response will not match the GS's model, and can result in instability in extreme cases. Should the GS' design not require feedback from the *connection point* measurements based on the model, longer communication detection times can be negotiated with the NSP and AEMO during the detailed design phase.
2. The GS must be equipped with a fail-safe mechanism that:
    (a) Automatically notifies the Operator of the communication loss and remains activated (latched) until it is Acknowledged by the Operator.

(b) Enables a shutdown command if the communication loss occurs twice within one hour or continues for more than 30 sec.

(c) Subject to paragraph (b), as PPC feedback quantities are not reliable during a communication failure, the PPC must command individual GUs (or groups of GUs) through the open loop system to ramp all GUs down to 0 MW and 0 MVar without relying on the *connection point* measurements.

(d) The GS' output must be automatically ramped down - without step or spike - before the shutdown to avoid sudden large changes in *active power*, *reactive power* or *voltage* at the *connection point*.

  (i) The ramping down period has to be approved by the NSP and AEMO but must not be longer than 5 min from the detection of the communication failure.

  (ii) Where the ramp function is not available on *active power* or *reactive power* at the *connection point*, the GUs (or groups of GUs) can shut down in a staggered manner to avoid sudden changes in quantities. For instance, if the first GU commences ramp down at time t and shuts down upon reaching zero output, the second GU must commence ramp down at t+X sec and shut down upon reaching zero output, the third GU must initiate ramping down at t+2X, and so on. X must be approved by AEMO and the NSP based on the size and number of GUs and the sensitivity of the *connection point* to the loss of a single GU and ramp rate limit of individual GUs. To avoid continuous and resonant oscillations, it is recommended that the X value is larger than the maximum observed *settling time* from the GS for the disturbance imposed by these shutdowns.

(e) The ramp down/up rate and the control mode of the GUs utilised for these responses must be approved by AEMO and the NSP and documented in the Communication Design Report.

(f) Once the GUs have ramped down to 0 MW and 0 MVar, they must shut down or *disconnect* from the grid.

(g) The GS must not ramp back up automatically upon recovery more than once for any two consecutive communication failures in an hour. The Operator must restart the GS manually once communication recovers, all relevant alarms are Acknowledged by the Operator, and AEMO and the NSP have approved the ramp up back to normal operation. This sequence is required to avoid potential oscillations caused by frequent bidirectional ramping.

4.3. Communication between PPC and GUs

This communication link is both Category 1 and Category 2. It can be broken, frozen or disturbed because of timed out handshaking between communicating elements, damage or changes to *network elements*, such as *network* switches or FOBOTS, disconnection of fibre or copper cables, failure in the media or protocol converters, loss of *supply* to *network elements*, timed out communication due to the high volume of the communication network traffic and many other reasons.

Such failures can disturb setpoint communications (or GU status) to the GUs from the PPC (or vice versa). This data delivery is required to prevent the GS from breaching the NER and unstable operation. These setpoints and statuses must be delivered within the time considered in the RMS and EMT models of the GS, which may include the discretisation of the PPC setpoints and transport delays.

Therefore, the GS's communication fail-safe mechanism must meet the following criteria:

(1) The PPC and GUs must detect the loss of communication within 500 ms and raise an alarm to the SCADA for the Operator to Acknowledge.

(a) This may be done using a default Watchdog bit available within the communication protocol or by customised logic that continuously monitors communication with the GUs.

(b) If there is a communication failure between the PPC and a single GU (or groups of GUs as specified by AEMO) and the failure is detected within 500 ms by the GU, raising a PPC alarm can exceed 500 ms if the communication failure detection algorithm is a function of the total number of lost packets from/to the PPC.

(c) As described in paragraph (2), the GU must initiate a self ramp down and shutdown but if it appears to be still operating, it must be manually shut down by the Operator in a staggered manner as described in paragraph (2).

(2) The GUs must also detect a communication loss within 500 ms and raise a latched alarm, which must:

(a) Automatically notifies the Operator of the communication loss and remains activated (latched) until it is Acknowledged by the Operator.

(b) Enables a shutdown command if the communication loss occurs twice within one hour or continues for more than 30 sec.

(c) Subject to paragraph (2)(b), the GUs must not change any setting and must only ramp to 0 MW and 0 MVar unless otherwise agreed under paragraph (e).

(d) The GS' output must be automatically ramped down - without step or spike - before the shutdown to avoid sudden large changes in *active power*, *reactive power* or *voltage* at the *connection point*.

i. The ramping down period has to be approved by the NSP and AEMO but must not be longer than 5 min from the detection of the communication failure.

ii. Where the ramp function is not available on *active power* or *reactive power* at the *connection point*, the GUs (or groups of GUs) can shut down in a staggered manner to avoid sudden changes in quantities. For instance, if the first GU commences ramp down at time t and shuts down upon reaching zero output, the second GU must commence ramp down at t+X sec and shut down upon reaching zero output, the third GU must initiate ramping down at t+2X, and so on. X must be approved by AEMO and the NSP based on the size and number of GUs and the sensitivity of the *connection point* to the loss of a single GU and ramp rate limit of individual GUs. To avoid continuous and resonant oscillations, it is recommended that the X value is larger than the maximum observed *settling time* from the GS for the disturbance imposed by these shutdowns.

(e) The ramp down/up rate and the control mode of the GUs utilised for these responses must be approved by AEMO and the NSP and documented in the Communication Design Report.

(f) Once the GUs have ramped down to 0 MW and 0 MVar (or the safe limit approved in the Communication Design Report), they must shut down or *disconnect* from the grid.

(g) The GUs must not ramp up the generation automatically upon recovery more than once for any two consecutive communication failures within one hour. The Operator must restart the GS manually once communication recovers, all relevant alarms are Acknowledged by the Operator, and AEMO and the NSP have approved the ramp up back

to normal operation. This sequence is required in order to avoid potential oscillations caused by frequent bidirectional ramping.

4.4. Communication between GUs and Measurement Unit

This communication link is a Category 1. It can be broken or disturbed because of failure in the installation of CT/VT connection to a GU meter, a broken link between the meter and the GU or failure of the GU's communication firmware.

This link usually transfers the GU's terminal power quantity measurements, which can include control loop feedback such as *voltage*, current, *frequency*, *active power* and *reactive power*. This feedback is critical for preventing the GS from breaching the NER and for stable operation of the GUs.

Therefore, the GS' communication fail-safe mechanism must meet the following criteria:

(1) A communication loss must be detected within 100 ms and raise an internal latched alarm within the GU and its control platform.

(2) It must notify the Operator of the communication loss and remain activated until Acknowledged by the Operator.

(3) It must enable shutdown or *disconnection* following the GU's ramping down to 0 MW and 0 MVar output if the communication loss occurs twice within one hour or once for longer than 30 sec.

(4) If the GUs cannot freeze the last received setpoints and measured values, the GUs must immediately shut down to avoid any potential oscillatory behaviour.

(5) The GUs must not ramp up generation automatically as soon as the communication status becomes healthy more than once for any two consecutive communication failures within one hour. GU restart must occur manually once the communication recovers and all alarms are Acknowledged by the Operator. AEMO and the NSP may be required to provide their approval prior to ramping back up the GU.

4.5. Communication Between PPC and Substation Equipment

This communication link is both Category 1 and Category 2. It can be broken or disturbed due to wrong installations in *substation* wiring, high volume of communication traffic and PPC and *substation* RTU firmware failure.

Loss of communication can impact the following signals that are transmitted between AEMO's/ NSP's *control centres* and the GS. A failure in the communication system between the GS' PPC and any *substation* controller (or within a *substation control system*) or SCADA equipment may stop updating key signals, such as:

- AEMO semi-dispatch SCADA signal
- Voltage setpoint
- VDS setpoint
- All the SCADA items in ECM used for forecasting purposes.
- Status of circuit breakers and auxiliary plant.
- Active and passive filter control and monitoring signals.
- Statuses from *substation* protection relays.
- Runback and inter-tripping signals.

The impact of the communication loss for signals may differ from one to another. For example, in the case of semi-dispatch GUs, if the SCADA data is bad, SCADA is not working as expected, not configured correctly, or doesn't represent actual conditions, the forecast accuracy will be impacted, which will result in discrepancies between the GS' *dispatch* target and actual output. If *Generators* fail to manage this, it can result in higher 'causer pays' factors for their portfolio. On the other hand, missing a *voltage* setpoint or a critical status could result in a breach of the NER, such as exceeding *rise time*, *settling time* or damping criteria or cause unstable operation.

Therefore, while the GS must comply with the Power System Data Communication Standard and the NSP Operational Protocol, the GS' communication fail-safe mechanism must meet the following criteria:

(1) This communication failure is detected within 5 sec (subject to no special impact identified by AEMO or the NSP) and raises a latched alarm to the GS' *control system* that notifies the Operator of the communication loss until Acknowledged by the Operator.

(2) Enables a shutdown command if the communication loss occurs twice within one week or continues for more than 5 min. In the event of planned *outages* for the routine maintenance activities by the *Generator* or the NSP, this shutdown command can be bypassed once approval from NSP and AEMO is granted.

(3) The GS must not ramp up generation as soon as the communication status becomes healthy more than once for any two consecutive communication failures within 15 min. The Operator must restart the GU manually once the communication recovers and all alarms are Acknowledged by the Operator.

APPENDIX A.

Figure 1. Generic communication layout raw file.

Figure 1.docx