Rod Hughes Consulting Pty Ltd
A.B.N. 64 137 442 089
7 Mulberry Grove
Aberfoyle Park
SA 5159
Australia
www.rodhughesconsulting.com

21 December 2022

AEMC
PO Box A2449
Sydney South
NSW 1235
Australia

Dear Sir/Madam

Proposal for additional definitions in the NER

This submission is to propose additional Glossary definitions to the NER (as currently at v191) and respective clause amendments in respect of certain protection related aspects of Schedule 5.1 and 5.2.

1. Imperative for change to the NER.

Since the inception of the NER, the industry has grappled with, in some cases, lack of clear "finite detail" definitions for certain protection system related terms and clauses. The industry at large has had a constant debate, conjecture **and potential mis-application of the intent of the NER**.

Even the CIGRE Australia industry association's "B5 Protection and Automation" Panel has, as I can personally attest to, had many such debates since NER v1 continuing even to this day and recent projects with no absolute consensus. The B5 Panel is constituted of arguably the "top" 30 or so protection specialists amongst the Australian utilities, suppliers, academics and consultants. Their collective expertise and opinions are highly regarded as "authoritative" on protection application principles, yet on the following matter they are at least "varied" in opinion.

I believe the addition of the proposed definitions and changes will lead to more clarity of the NER and **lead to correct implementation of the intent of the respective clauses**.

2. Relevant clauses

The words/phrases highlighted in red below are critical to the detailed design as well as the safe, reliable and secure operation of the protection system, and hence to the power system overall.

However, these highlighted words/phrases are not currently defined in the NER.

- Schedule 5.1 Network Performance Requirements to be Provided or Co-ordinated by Network Service Providers
  - S5.1.9 Protection systems and fault clearance times

    (c) ... must provide sufficient primary *protection systems* and back-up protection systems (including *breaker fail protection systems*) to ensure ...

    (d) ... the primary protection system must have sufficient redundancy to ensure ...

    (f) The fault clearance time of each breaker fail protection system or similar back-up protection system ...

- Schedule 5.2 Conditions for Connection of Generators
  - S5.2.5.9 Protection systems that impact on power system security

    (a) (2) each primary protection system must have sufficient redundancy ...

3. Semantic Issues

The following represents several semantic interpretations without necessarily implying any specific agreement or dispute on the part of myself to those views. They are to merely provide an indication of the extent of variation and debate observed in the industry over the past 30 or so years to which I believe can be eliminated.

3.1. "primary" and "back-up"

The NER Glossary currently defines the following terms

breaker fail protection system

protection system

secondary equipment

However, the term "primary" in the context of protection systems is not defined.

Whilst *breaker fail protection system* is referenced in S5.1a.8 (d) as being similar to "back-up" protection systems, other "back-up" possibilities exist but are not defined or inferred by an all-encompassing definition of "back-up".

3.2. "sufficient redundancy" and "ensure"

The NER phrase in question is:

S5.1.9 (d) ... must have sufficient redundancy to ensure ...

- *S5.2.5.9 (a) (2)* ... must have sufficient redundancy to ensure ...

The word "redundancy" has as one meaning as "not needed". This is the exact opposite of the intention that it is essential in order to "ensure". Furthermore, the inclusion of the word "sufficient" is far from giving any meaningful guidance to the industry or enforcement by AEMO.

The lack of clarity in this phrase is evident as follows.

The industry at large would generally say that "redundancy" of the protection system is commonly achieved by duplication of the entire protection system comprising:

- CT cores
- VT windings
- Relays
- Auxiliary/tripping d.c. batteries
- Battery chargers
- Auxiliary a.c. auxiliary supply to the chargers
- Trip coils
- Wiring
- Communication systems upon which the protection system relies

Some would also argue total physical segregation of those components to maintain independent operation secure from any common mode of failure to the extent of separate/partitioned cubicles, wire routing etc..

This duplication (and segregation) is to ensure that there is no (single) mode of failure that would prevent at least one of the redundant system from operating.

However, in the context of "sufficient" and "ensure" (the latter having the meaning of "never not so"), a single or series of "catastrophic" multiple failures could still result in both of the duplicate systems failing to operate and hence failing to ensure the fault is cleared.

It can be seen that "sufficient" and "ensure" implies as many number of systems as necessary such that the fault will always be cleared regardless of how many contingent system failures occur. This is both in terms of design, and in post event forensics.

In other words, in extreme circumstances, if both of the fully duplicate systems fail to clear the fault as required, "sufficient redundancy" has not been achieved, and the participant is still in breach of the NER despite having fully duplicated systems!

Due to the abstract nature of having "sufficient redundancy", even "inverting" the terminology as follows provides no clear guide on implementation as the elements of required proof is equally undefined.

> *Non-redundant systems can be implemented if it can be proven that a single failure of anything in the protection system will not prevent the system from automatically clearing a fault of any fault type anywhere on its transmission system or distribution system in accordance with clause S5.1.9(e) or clause S5.1.9(f)*

In consequence of the lack of specific definition of "primary", "back-up" and "sufficient redundancy", a common implementation of general redundancy for two protections seeing a fault is the use of protection systems at two different locations or in respect of two different but at least partially "overlapping" zones of the power system. Examples of such "redundant" systems include:

- the outgoing feeder of a busbar and one on the incomer to the same busbar
- the incomer overcurrent protection relative to specific bus bar differential protection
- the high voltage side overcurrent protection and the transformer differential protection
- an unrestricted earth fault function and a restricted "winding earth fault" function

In each of these examples, there is one protection system that is **intended to operate first** in order to detect the fault with maximum sensitivity, operate as fast as appropriate to the circumstances and trip the least number of circuit breakers closest to the fault in order to clear the fault. The other protection system has different operation in one or more respects of:

- Faults occurring in different locations,
- Less sensitivity to the fault (higher operating thresholds),
- Slower operation,
- Different circuit breakers operating to clear the fault,
- Failure of an individual element of the two systems prevents operation of both

In each case there may be at least one common mode of failure between these systems. , e.g. arguably the most common as the same auxiliary supply to both locations of "incomer and outgoer" or "high and low voltage" sides of a transformer protection systems. Therefore, none of these scenarios fall under the principles of "sufficient redundancy" and "ensure" in respect of clearing any particular fault", but they are examples that are often referenced as being "sufficiently redundant" and hence are in common use.

3.3. "primary" vs "main" protection systems

The word "primary" itself presents a semantic conflict in the context of a power grid as often referring to the electricity grid itself. Ironically, this could be a correct interpretation in these clauses as the protection system does protect the power grid as the primary system!

Indeed, the NER Glossary itself defines "*secondary equipment*" as assets *"... including protection...*" and hence is at least conflicting with the reference to a "primary protection system".

In this context of the above clauses, it is evident that the word "primary" is inferring the definition as the "main or principal" function compared to a back-up, e.g. as dictionaries would define:

of chief importance; principal

earliest in time or order

This recommendation is therefore to change the word "primary" to the word "main" in order to eliminate the semantic conflict and more directly be related to "main and back-up" concepts. An alternative could be "principal" but is not commonly used in the industry in this context which would likely lead to further confusion.

The word "main" is also consistent with common industry terminology for duplicate (i.e. redundant) protections systems – the industry often tags these as "X and Y", "No1 and No2", or more explicitly as "Main 1 and Main 2".

The use of "main" instead of "primary" is also consistent with various domain-text books such as the Schneider Network Protection & Automation Guide which is considered one of the top text books on implementing protection systems dating back to the 1960's. (https://www.se.com/ww/en/tools/npag-full-online-unlocked-1130re14y/)

The Schneider NPAG states in Section A1, Chapter 9:

> *The reliability of a power system has been discussed earlier, including the use of more than one primary (or 'main') protection system operating in parallel. In the event of failure or non- availability of the primary protection some other means of ensuring that the fault is isolated must be provided. These secondary systems are referred to as 'back-up protection'.*

Similarly, the Electricity Supply Association of Australia "Power System Protection" (1996) text book (ISBN 1 86272 473 3) "Recommended Terminology" states:

> *Main Protection* — *A protection system expected to have priority over back-up systems in initiating fault clearance*

3.4. Definition of back-up protection systems

Example Definition that CBF is one form of back-up

The Schneider NPAG infers back-up protection is

> *some other means of ensuring that the fault is isolated in the event of failure or non- availability of the primary protection*

The ESAA text book referenced above states as "Recommended Terminology":

Back-up Protection	*A protection which is intended to operate when a system fault is not cleared in due time because of a failure or inability of the main protection or the associated circuit-circuit breaker to operate*

3.5. Definition of breaker failure protection systems protection systems

The ESAA text book referenced above also states as "Recommended Terminology":

Breaker Failure Protection	*a specific form of local back-up protection which operates in the event of a circuit breaker failing to clear a fault and trips all other circuits feeding into the same section of busbar as that breaker*

3.6. "sufficient redundancy" vs "independent alternative"

The intent of "sufficient redundancy" is to build in a level of assurance of operation via some (at least two) alternate means to clear the fault. The intent is also that these (at least two) alternate means are totally independent of each other such that there is no (reasonably credible) single mode failure that would prevent the fault being cleared by at least one system.

Clarity of this intent is established by replacing "sufficient redundancy" with "independent alternatives"

Importantly, this does not specifically prescribe duplication. This is at least relevant to the last reference in **S5.1.9 (d)** where "sufficient redundancy" is required:

"including any communications facility upon which the protection system depends"

Since the NER inception, this clause has for shadowed and catered for such evolutions from the somewhat basic limited communication reliance at the time.

Modern protection systems are more and more based on Ethernet technology in almost every respect, e.g. today's reality of the "digital substation".

Along with that reliance on the communication system, undoubtedly there has been significant advancements in reliability of Ethernet technologies used in the protection equipment (e.g. IEC 62439-3 Parallel Redundancy Protocol and High-availability Seamless Redundancy). This is to the extent that whilst the protection systems themselves are duplicated; such Ethernet technology allows the two protection systems to share a common communication infrastructure. The devices simultaneously send and receive messages via two alternative paths. Hence the failure of one path does not disrupt the "communications upon which the protection system relies".

Therefore further duplication of such communications infrastructure is superfluous to the intent of "sufficient redundancy" and the resilience of the system to continue to operate correctly with any one element out-of-service.

3.7. Just the connection point

Of course, there are many forms of Proponent power systems "below" the Connection Point. Naturally there is no specific protection of "*the* Connection Point", however many Proponents claim the reference is only to the **first protection system** on the Proponent's side of the Connection Point based on the following clause.

> *S5.1.9 (a) A Network Service Provider must determine the automatic access standard and minimum access standard that applies to the protection zone of each protection system in relation to the connection point and the plant to be connected, ...*

As an example, they may be a Connection Point at a certain high voltage level, a step-down transformer and a lower voltage level power system (or perhaps a step-up in the case of a generator).

In such cases, it is claimed that the requirement for "sufficient redundancy" only applies to the transformer protection as the first protection scheme of the "connected plant" below the Connection Point. This leaves the entire lower voltage network as only provisioned with non-redundant primary protection, albeit one primary and some level of "back-up" protection.

It is also possible to put a case that such non-redundant protection below the Connection Point has to be validated by the proponent and verified by AEMO/NSP under the "ensure" requirement as NEVER being ABLE TO, and NEVER ACTUALLY causes a power system stability/security issue, even beyond the first plant being connected.

However, the NER Chapter 10 Glossary provides the definition of plant as

> *plant (a) In relation to a connection point, includes all equipment involved in generating, utilising or transmitting electrical energy.*

Hence in the case of a generator of any technology/fuel source, the NER therefore stipulates sufficient redundant protection for all equipment from the generator of the electricity to the Connection Point.

Furter it also infers all protection of any equipment using electrical energy below the Connection Point.

In an extreme sense, the NER could be interpreted as demanding even down to the 400 V consumer network that there must be "the primary protection system must have sufficient redundancy to ensure ...". The "escape clause" on that extreme interpretation is that it is fundamentally not possible for a 400 V system fault to impact power system stability/security at the much higher voltage levels.

However, at higher voltage levels there seems to be an implication of the ensure provision to undertake somewhat extensive fault studies of the non-operation of non-redundant primary protection systems.

4. Proposed Additional/Changed Glossary Definitions

The NER already has definition for "*breaker fail protection system*" (although recommended to be modified as below), so there is consistency to define additional protection-related terms based on the above change from "primary" to "main".

back-up protection system (new)

> A *protection system* that operates in consequence of a *main protection system* having failed to clear the fault in its expected time. The back-up protection system will have time and/or measurand grading to the *main protection system*. A back-up protection system may be itself a *main protection system* for other fault scenarios.
>
> A *back-up protection system* is not an *independent alternative main protection system* as it may share common modes of failure to the *main protection system* (e.g. auxiliary supply) and/or may not be as sensitive and/or as fast as the *main protection system* so as to clear all faults in a similar time frame as expected to be cleared by the *main protection system*.
>
> Examples of *back-up protection systems* include breaker fail protection systems as well as other *main protection systems* located at other points in the power system with different time and/or measurand settings.

breaker fail protection system (change)

> A *protection system* that, upon detecting failure of its monitored circuit breaker to clear the fault following operation of the *breaker fail protection system*'s respective *independent alternative main protection system*, operates to directly open other required circuit breakers to clear the fault independently of any other *protection function* operation.

control function (new)

> A function associated with the normal operation in absence of a power system fault that may be required to manage, monitor or control the power system performance and/or correct an abnormal condition of the power system.

independent alternative main protection system (new)

> A *main protection system* that operates with similar measurand value sensitivity and speed of operation as another *main protection system* such that it is generally expected that both would be able to operate in approximately the same time for the same fault. Specifically there must be no credible mode of failure or out-of-service condition of any of the respective *protection elements* such as to prevent correct operation of both systems for a particular fault.

main protection system (new)

> A *protection system* that is the intended and preferred system to clear a fault in order to minimise the number of required circuit breakers to clear the fault as close as possible to the fault.

protection element (new)

Any of the facilities, equipment, physical and virtual connections of the *protection system* including: CT cores, VT windings, Trip coils, devices providing *protection functions*, Auxiliary/tripping d.c. batteries, Battery chargers, Auxiliary a.c. auxiliary supply, Wiring, Communication systems.

protection function (new)

A function that is intended to operate on the basis of a fault or other excessive operating condition of the power system.

5. Proposed clause changes

In consequence of the above word/phrase changes and new/updated definitions, the affected clauses could be re-presented as follows:

- Schedule 5.1 Network Performance Requirements to be Provided or Co-ordinated by Network Service Providers
  - S5.1.9 Protection systems and fault clearance times

    (c) Subject to clauses S5.1.9(k) and S5.1.9(l), a Network Service Provider must provide *alternative main protection systems* and *back-up protection systems* (including *breaker fail protection systems*) to ensure that a fault of any fault type anywhere on its transmission system or distribution system is automatically disconnected in accordance with clause S5.1.9(e) or clause S5.1.9(f).

    (d) If the fault clearance time determined under clause S5.1.9(e) of a *main protection system* for a two phase to ground short circuit fault is less than 10 seconds, *alternative main protection systems* must be provided to ensure that short circuit faults of any fault type can be cleared within the relevant fault clearance time with any single *protection element* out of service ...

- Schedule 5.2 Conditions for Connection of Generators
  - S5.2.5.9 Protection systems that impact on power system security

    (a) (2) alternative main protection systems must be provided to ensure that a faulted element within its protection zone is disconnected from the power system within the applicable fault clearance time with any single protection element out of service ...

6. Contribution to the National Electricity Objective "NEO"

Reliability and Security of the power system are key principles of the NEO.

Correct isolation and clearance of faults is a fundamental requirement such that any uncleared or slow clearance of the initial fault

1. Will not undermine power system stability,
2. Will not perpetuate and expand consequential damage to the power system equipment and other facilities,
   and of course,
3. Will not exacerbate the extent of consequential injury or death.

Correct fault isolation cannot be achieved if the protection system fails to operate reliably operate, and hence the NEO will not be met in one or more respects.

The concept of "reliability" includes the principles of Dependability and Resilience

- Th system will do what it has to do when it has to do it
- The system will continue to do what it has to do with one part of the system out of service for any reason

7. Potential impacts of this change to the Rules

The clarification of these terms and clauses will undoubtedly be of concern to a significant part of the community, particularly those that have implemented their protection systems based on the various examples provided above as *supposedly* complying with the NER, at least as they have chosen to define the terms.

On the other hand, clear definitions (these proposed or other) will eliminate such wasted engineering debate on ad hoc interpretations, thereby lowering the cost of implementation of an electrical project.

This proposal reflects my professional opinion of the necessary changes to the NER based on my observations and involvement over "30 years" in many discussions and debates about the application of the referenced clauses of the NER. There may of course be other opinions or interpretations which may significantly different/opposite to my views expressed here and/or be equally or more appropriate.

I remain willing to participate any further refinement of these terms and clauses for the betterment of the application of the NER throughout the industry and improved engineering, performance, reliability and security outcomes.

I trust that this proposal is sufficiently explained to enable your consideration and possible implementation.

However, in the event that you have further questions, please do not hesitate to contact me by email and or phone at your convenience.

Sincerely

Rodney Hughes
Managing Director
Email: rgh@rodhughesconsulting.com
Mobile: +61 419 845 253