Pilbara ISOCo
Independent System Operator

ISSUES PAPER:

REVIEW OF SUBCHAPTER 7.3 AND 7.4 OF THE PILBARA NETWORKS RULES

19 JULY 2024

TABLE OF CONTENTS

TABLE OF ISSUES

		Page
Issue 1.	Subchapters 7.3 and 7.4 do not specify the "system security objective" as their primary objective.	12
Issue 2.	The emphasis on informality and collaboration has resulted in processes under Subchapters 7.3 and 7.4 that lack rigour. It has been suggested that the Pilbara outage management regime should copy the WEM Rules'.	13
Issue 3.	The definition of "notifiable event" is very broad. The Subchapter 7.3 and 7.4 processes may need to differentiate between, and integrate across, different classes of notifiable event, for example: • planned maintenance and routine upgrades; • major or extended outages; • commissioning and testing; • events in integrated mining networks; • events in the Pluto facility; and • events in another connection point compliance facility.	14
Issue 4.	Under the current rules, a planned outage is a contingency, and not a pre-contingent threat, and so falls to be managed under rule 187 which has a focus on reactive post-contingent responses.	17
Issue 5.	Because a planned outage is a contingency, whenever a planned outage is occurring anywhere in the NWIS, the system is defined to be "outside normal operating conditions", enabling relevant protocols to be activated (if their activation conditions are met)—but the pre-contingent protocol will *not* be available. The ISO seeks stakeholder feedback on whether this is a desirable outcome, or whether: (a) planned outages would be better managed as a variety of pre-contingent threat; or (b) the definition of "normal operating state" should be changed so that the system can (or can sometimes) remain in this state despite planned outages being under way; or (c) a fourth operating state is required, specifically to deal with planned outages.	17
Issue 6.	The rules rely primarily on oral discussion as the means for NSPs to notify the ISO and other NSPs of notifiable events. This minimises the compliance burden for near-term coordination, but may not be the optimum way to manage scheduling and assessment (including modelling) for outages which are known well in advance.	18
Issue 7.	There is no Procedure regarding outage management and the rules do not provide for one.	19

Issue 8.	The rules regarding the composition, agenda and duration of system coordination meetings are too prescriptive. These matters may be better located in a Procedure.	19
Issue 9.	The rules do not clearly allocate responsibility for determining the impacts a notifiable event might have on the power system, including security, reliability, constraints and ESS, or for the risk and other analysis and modelling required to assess these things, and do not provide a mechanism for accommodating different risk appetites or resolving disagreements on these matters.	20
Issue 10.	If there is disagreement between Horizon Power and another NSP regarding the assessment of a notifiable event, the ISO's use of ISO control desk staff to help in the assessment places a focus on how Horizon Power manages the staff's conflict of interest.	20
Issue 11.	There is no general requirement for planned outages and other notifiable events to be approved.	20
Issue 12.	Except in the case of a scheduling conflict, the rules to not provide for a notifiable event to be stopped or deferred, or otherwise be the subject of a direction, pending satisfactory resolution of any disagreement regarding its impacts on other participants, e.g. by way of its impact on security, reliability, constraints or ESS.	21
Issue 13.	The definition of scheduling conflict is limited to events which may take the system outside the technical envelope or otherwise pose an unacceptable risk to security or reliability. This does not require the system to be maintained in a secure state, and does not assess other impacts such as on risk, constraints, ESS or cost.	22
Issue 14.	The ISO's power to intervene in a scheduling conflict is not enlivened until it has first determined that a consensus is unlikely to be reached in time. This could create system risk.	22
Issue 15.	Are the ISO's direction powers under rules 182(3) to (5) appropriate and sufficient?	22
Issue 16.	The rules do not deal with how network planning criteria are to be dealt with in assessing, managing and mitigating notifiable events.	23
Issue 17.	The rules and protocols do not deal cleanly with a situation in which islanding has not yet occurred but pre-contingent actions are necessary, e.g. to prevent islanding or ensure the island is secure (or at least inside the technical envelope) should islanding occur.	24
Issue 18.	There is no clear mechanism for identifying the measures necessary to manage or mitigate a notifiable event, and no clear obligation on any person to implement those measures once identified.	25
Issue 19.	There is no practicable mechanism to resolve differences of opinion in connection with notifiable events, for example regarding risk assessment and how or by whom a notifiable event is to be mitigated or managed.	25
Issue 20.	A question has been raised as to whether there should be any exemption from rules participants' system security obligations during a notifiable event.	25
Issue 21.	The rules do not deal separately with the specification and procurement of, and cost recovery for, additional ESS, or machine start or other services, when this is required	26

	to manage or mitigate a notifiable event, rather than as part of normal system operations under Chapter 8.	
Issue 22.	The ISO has no power to direct how a notifiable event is to be managed or mitigated.	27
Issue 23.	The nature and timing of pre-contingent powers required to manage notifiable events are likely sufficiently different to the post-contingent powers the ISO control desk needs to manage contingencies, that it is appropriate for them to be exercised by the ISO rather than the ISO control desk. The current pre-contingent protocol was not designed to manage notifiable events.	27
Issue 24.	The rules lack any mechanism to determine and apportion the costs of managing and mitigating notifiable events. A choice needs to be made as to whether mitigation costs should be apportioned on a causer pays, beneficiary pays or socialised basis, or some combination of these or some other basis.	28
Issue 25.	The regime for notifying, assessing, managing and mitigating notifiable events must appropriately balance transparency, accountability, confidentiality and competition.	29
Issue 26.	If the ISO is given an expanded role to address the issues identified in this paper, it would have resourcing and hence cost implications.	29

1. Introduction

1.1 Purpose of this Issues Paper

1.1.1 A primary goal of the Pilbara regime[1] is to maintain and improve power system security.[2] Chapter 7 of the Rules deals with the main operational aspects of this, and one important component of Chapter 7 is the processes set out in Subchapters 7.3 and 7.4 for notifying, assessing, coordinating and managing planned and unplanned outages and other "notifiable events".[3]

1.1.2 Rule 178 requires the ISO periodically to conduct a review of Subchapter 7.3 and 7.4's processes against the "Pilbara electricity objective".[4] This Issues Paper forms the first formal step in that review.

1.1.3 The ISO seeks feedback from stakeholders on:

(a) the processes for identification, notification, assessment and approval of notifiable events;

(b) the process for determining how and by whom a notifiable event is to be managed or mitigated, including:

(i) how the system is to be configured and operated, and how contingencies are to be identified and managed, during the notifiable event; and

(ii) the role and effectiveness of the protocol framework;

(c) the roles, responsibilities and accountability of registered NSPs, registered controllers, the ISO control desk and the ISO including transparency and confidentiality requirements; and

(d) the allocation of costs associated with the management and mitigation of notifiable events.

1.2 The legislative framework

IMPORTANT NOTICE: For readability, this paper generally gives simplified narrative descriptions of Rules and other instruments. Please refer to the published Rules and Procedures for the exact wording.

[1] Implemented under Part 8A of the *Electricity Industry Act 2004*, and including the *Electricity Industry (Pilbara Networks) Regulations 2021*, the *Pilbara Networks Access Code*, *Pilbara Networks Rules*, *Harmonised Technical Rules* and various procedures made under the Rules.

[2] *Electricity Industry Act 2004* sections 119(1)(c), 119(2), 120K(1) and (2), and 120W(4)(a)

[3]119(2) A "notifiable event" is any planned or anticipated outage or other system event which might credibly be expected to adversely effect power system security, the delivery and effectiveness of essential system services, or the ability of covered transmission NSPs to provide contracted access services: Rule 166.

[4] Section 119(2) of the Electricity Industry Act 2004 sets out the Pilbara electricity objective:

> *"… to promote efficient investment in, and efficient operation and use of, services of Pilbara networks for the long-term interests of consumers of electricity in the Pilbara region in relation to —*
>
> *(a) price, quality, safety, reliability and security of supply of electricity; and*
>
> *(b) the reliability, safety and security of any interconnected Pilbara system."*

1.2.1 Part 8A of the *Electricity Industry Act 2004* provides the statutory basis of the Pilbara regime, and sets out the Pilbara electricity objective and the ISO's core functions, which include maintaining and improving power system security in the NWIS.[5]

1.2.2 Part 8A of the Act empowers regulations (the *Electricity Industry (Pilbara Networks) Regulations 2021*) which in turn empower the making of rules including the *Pilbara Networks Rules*.

1.2.3 In turn, the *Pilbara Networks Rules* empower the ISO and others to make *Procedures* to supplement the Rules including, importantly, the *Protocol Framework Procedure* which sets out the *Protocols* by which the ISO Control Desk and NSPs are to manage contingency events and other matters which may threaten power system security.

1.3 Experience to date

1.3.1 Since commencement of the processes under these Subchapters there have been a number of notifiable events. Notifiable events that have occurred since 1 July 2023 are briefly summarised in the system coordination bulletins published on the ISO's website in accordance with rule 288.[6]

1.3.2 Some stakeholders have been dissatisfied with Subchapter 7.3 and 7.4 processes and outcomes in respect of some of these previous instances.

1.3.3 However, this review is prospective. It is not the function of this review to report on or analyse specific past instances or outcomes, although of course experience from those past instances has informed some of the issues identified below, and (subject to the requirements of confidentiality discussed in section 2.4 below) stakeholders are welcome to illustrate their submissions by reference to past instances.

1.4 EPWA's governance review

1.4.1 As part of its *Evolving the Pilbara Networks Rules* (EPNR) project, EPWA is undertaking a wide-ranging review of the Pilbara regime's governance.

1.4.2 There is clearly some overlap between the issues addressed by this rule 178 review and EPWA's EPNR Governance review, although the EPWA review will be broader.

1.4.3 The ISO plans to liaise with EPWA during this rule 178 review, to ensure that stakeholder feedback is addressed in the most appropriate forum, and to minimise any duplication of effort.

1.4.4 At a high level, the ISO considers the following to be matters predominantly for the EPNR Governance review:

(a) The composition of entities, including vertical integration of NSPs and Pilbara ISOCo Ltd's membership and internal governance.

[5] *Electricity Industry Act 2004*, section 120W(4)(a).

[6] Available here.

(b) The ISO's funding arrangements.

(c) The delegation of the ISO control desk function to Horizon Power[7] and Horizon Power's internal governance regarding that function (except as discussed in paragraph 5.5.6 below).

(d) The rules' general (i.e. outside Subchapters 7.3 and 7.4) emphasis on collaboration and consultation, rather than prescription.

(e) The specification and procurement of, and cost recovery for, essential system services (**ESS**) under Chapter 8 of the rules.

[7] The rules permit, but do not require, the ISO to delegate the control desk function: rule 45.

2. Consultation Process and Timeline

2.1.1 Under rule 178, as part of this review the ISO is required to consult with registered NSPs, registered controllers and undertake public consultation following the expedited consultation process set out in rule A1.3. At the conclusion of the review, the ISO must publish a report containing any recommending changes to Subchapters 7.3 or 7.4 or the associated procedures.

2.1.2 Public consultation is an important part of the ISO's transparent decision-making process, and the ISO welcomes stakeholder feedback on this Issues Paper or otherwise in relation to the processes set out in Subchapters 7.3 and 7.4 and the associated Procedures. All consultation will be undertaken in accordance with the ISO's *Consultation Policy*.[8]

2.1.3 The ISO will take into account all in-time submissions and other comments. It will endeavour where practicable to consider late submissions.[9] If you have missed a submission deadline but feel you have an important contribution to make, please contact the ISO promptly at info@pilbaraisoco.com.au.

2.1.4 The ISO is working to the following timetable:

Event	Date	Comments
Issues Paper	19 July 2024	Complete
Informal consultation	22 July 2024 – 9 August 2024	The ISO wishes to conduct this first round of stakeholder feedback as informally as possible, see section 2.2 below (rule A1.3(a)).
Draft decision	16 August 2024	The ISO will publish the draft decision together with a notice inviting written submissions and comments (rule A1.3(b)).
Formal written consultation	19 August 2024 – 7 September 2024	The ISO will allow a period of at least 15 Business Days for written submissions and comments on the draft decision (rule A1.3(b)).
Final decision and publication of report (rule 178(3))	Target late September 2024	Final decision is to be within 20 Business Days after the end of the period allowed for making submissions and comments on the draft decision (rule A1.3(c)).

2.2 First round of consultation (now) – informal feedback

2.2.1 The expedited consultation process required by rule 178(2) provides for one round of formal written submissions, after the ISO publishes a draft decision. Before the draft decision, the ISO may consult as it considers appropriate.[10]

2.2.2 The ISO wants to make participation in this review as non-burdensome as possible, and accordingly would prefer to obtain stakeholder feedback on this Issues Paper through informal communications and discussions.

[8] Available here.

[9] Under rule A1.6, the ISO may, but does not have to, take into account out-of-time submissions.

[10] Rule A1.3(a)

2.2.3 The ISO is willing to meet with any stakeholder to discuss this Issues Paper. Please contact the ISO at info@pilbaraisoco.com.au if you wish to arrange a meeting, or email your feedback to submissions@pilbaraisoco.com.au.

2.2.4 This first round of feedback will allow the ISO to refine the issues and form preliminary views on possible solutions. It will publish these in the draft decision.

2.3 Second round of consultation (later) – Written submissions and comments

2.3.1 Once the draft decision is published, the ISO will invite stakeholders to provide written submissions or comments (rule A1.3(b)(ii)). Stakeholders will have at least 15 business days for this.

2.4 Confidentiality and transparency

2.4.1 This review will consider whether any changes might be required to the rules' confidentiality and transparency regimes (see section 7 below), but for the time being, stakeholders are reminded of the regime's existing rules regarding confidentiality.[11]

2.4.2 The ISO's preference is for this review and associated stakeholder feedback to be as transparent as possible. Generally, written submissions received will be published on the ISO's website,[12] and the ISO will endeavour to reflect all relevant informal feedback in its draft decision.

2.4.3 However, the ISO recognises that a stakeholder may wish to provide confidential information or make a confidential submission, in which case:

(a) please clearly identify to the ISO which parts of any submission or feedback are confidential;

(b) wherever possible please refrain from making blanket claims of confidentiality over an entire submission;

(c) for any written submission, please also provide a redacted version for publication; and

(d) the ISO will deal with any claims of confidentiality in accordance with rules A1.8 and A1.9.

2.5 Further Information

2.5.1 If you require any further information, please contact us at info@pilbaraisoco.com.au.

[11] Subchapter 11.2, also rule 176 and rules A1.8 and A1.9.

[12] Rule A1.5

3. History and design philosophy

3.1.1 Before the Pilbara regime commenced in 2021, the NWIS had operated moderately successfully through largely unregulated collaborative activity by the three primary NSPs. The arrangements and outcomes were neither perfect nor necessarily the most efficient but, in general, historical operational practices on the NWIS achieved tolerable levels of reliability and security most of the time.

3.1.2 The 2021 reforms recognised this reality. They sought to preserve the best of the past (informality, collaboration and generally low compliance costs) while imposing more transparency and more rigour on matters relating to third party access, and aiming for incremental improvements in security and reliability.

3.1.3 Part of this was the adoption of the cost-saving "administrative ISO" model, in which the control desk function is delegated to Horizon Power.

3.1.4 EPWA's EPNR review will reexamine some of these 2021 design decisions, to see whether they remain appropriate for the rapidly evolving and decarbonising Pilbara electricity landscape. That is not a matter for this review.

3.1.5 One of the ways in which the 2021 reforms did depart from past practices was to provide for clearer, more independent and more accountable decision-making in some areas such as technical exemptions connection approvals, the procurement of ESS and energy settlement, by empowering the ISO as a final determiner of these matters and providing some process machinery.

3.1.6 But this was not the case for the management of outages and other notifiable events.

3.1.7 Other regimes contain formal, detailed regimes for managing planned outages, in which the system operator has a central approval role.[13] The Pilbara rules, in contrast, adopt a very light touch approach to outage management, with an emphasis on NSP collaboration and self-determination.

3.1.8 Thus, in 2021 it was decided after considerable stakeholder consultation to leave outage management largely in the NSPs' hands, with the ISO's role being mostly facilitative. As rule 173(1) makes clear, Subchapters 7.3 and 7.4 seek to promote communication, collaboration and information exchange, and the collaborative resolution of any scheduling conflicts and similar matters. The ISO's powers to intervene were limited to making recommendations in the system coordination report,[14] and giving last-resort directions to resolve only scheduling conflicts, and only if collaboration has failed.[15]

3.1.9 This review invites stakeholders to comment on how this approach has worked in practice.

3.1.10 Whether the Rules' overall allocation of roles between the ISO and NSPs will remain fit for purpose in the evolving Pilbara grid is beyond the scope of this review. But this paper identifies some areas

[13] The outage management regime in the *Wholesale Electricity Market Rules* (**WEM Rules**) for WA's South-West Interconnected System (**SWIS**) is summarised here. A more detailed summary can be found in section 6.5 of AEMO's *Wholesale Electricity Market Design Summary* of September 2023, here. The National Electricity Market (**NEM**)'s network outage regime is summarised here, and more detail on outage management for all facilities can be found here.

[14] Rule 177(1)(c)

[15] Rule 182(3)

where experience with the outage management regime to date suggests that more intervention may be needed.

4. The objectives of Subchapters 7.3 and 7.4

4.1.1 Subchapter 7.1 defines the core "system security objective", and also sets out related definitions including what it means for the NWIS to be **"inside the technical envelope"**[16] (meaning all equipment is operating within normal parameters, and voltage and frequency are within normal bounds) and in a **"secure state"** (meaning that the system not only is inside the technical envelope, but is expected to remain so even after the worst single credible contingency).

4.1.2 The **"system security objective"** is:

(a) to keep the power system inside the technical envelope, and failing this to return it to that state "promptly";

(b) to keep the power system in a secure state, and failing this to return it to that state "as soon as practicable"; and

(c) otherwise to maintain and improve power system security and reliability.

4.1.3 Rule 173(1) provides that the primary objective of Subchapters 7.3 and 7.4 is to —

(a) promote communication and collaboration between the ISO and registered NSPs regarding "system coordination matters"; and

(b) in so doing provide the ISO, registered NSPs and ESS Providers with the information they reasonably need to perform their obligations under the rules and relevant contracts, with a view to achieving the system security objective; and

(c) promote the collaborative resolution of scheduling conflicts regarding outages and other system coordination matters.

4.1.4 Thus, Subchapters 7.3 and 7.4 do not adopt the system security objective as their primary objective. Rather, that objective emerges indirectly through rule 173(1)(b), as part of a collaborative approach to system coordination matters, and applied only to the provision of information.

4.1.5 The system security objective returns in Subchapter 7.5, where it provides one of the guiding objectives for each of NSPs and the ISO Control Desk,[17] but the ISO is not included in these provisions

Issue 1: Subchapters 7.3 and 7.4 do not specify the "system security objective" as their primary objective.

4.1.6 Rule 173(2) provides that the secondary objectives of Subchapters 7.3 and 7.4 are to pursue the primary objective in as efficient and informal a manner as practicable, maximising communication while minimising the compliance burden.

4.1.7 On their own, and as *secondary* objectives only, the ISO has not identified any issue with these objectives. The issues identified throughout this paper have to do with how these objectives of

[16] Rule 163. This is broadly analogous to what the NEM and the WEM call a "satisfactory operating state".

[17] Rules 185(1)(c) and 185(2)(c) respectively.

informality and collaboration have been codified in the rules, for example in rule 174 (system coordination meetings), the lack of a head of power to make a System Coordination Procedure, the lack of a formal risk framework, etc.

4.1.8 It has been suggested to the ISO that the Pilbara regime should adopt the formal outage management regime which has been developed in the *Wholesale Electricity Market Rules* (**WEM Rules**) for WA's South-West Interconnected System (**SWIS**).[18] The ISO invites stakeholder comment on this suggestion. The WEM Rules' regime offers a mature process which has recently been through extensive evolution and stakeholder consultation, and which is ready to scale as the NWIS grows more complex. The question is whether the NWIS presently needs this level of formality and its associated resource requirements.

Issue 2: The emphasis on informality and collaboration has resulted in processes under Subchapters 7.3 and 7.4 that lack rigour. It has been suggested that the Pilbara outage management regime should copy the WEM Rules'.

[18] The WEM Rules' outage management regime is summarised here and a more detailed summary can be found in section 6.5 of AEMO's *Wholesale Electricity Market Design Summary* of September 2023, here.

5. Identification and notification of notifiable events

5.1 Planned outages and other "notifiable events"

5.1.1 **"Notifiable event"** is defined broadly under rule 166, to include not only planned outages, but also any other planned or anticipated system event which might credibly affect system security or reliability, the provision of ESS, or the provision of contracted transmission access.[19]

5.1.2 Thus, while planned outages represent the most common focus of the Subchapter 7.3 and 7.4 processes, the regime is not limited to only planned outages.

5.1.3 One issue with this definition is the possible ambiguity or overlap with the definition of "pre-contingent threat" discussed at section 5.3 below.

5.1.4 Another issue is that "notifiable event" includes not only planned outages, but also commissioning and testing. While this is appropriate in the sense that commissioning and testing activities also need to be managed as system coordination matters, it's important that the Subchapter 7.3 and 7.4 processes accommodate the fact that commissioning and testing may require quite different treatment from other planned outages—for example regarding cost allocation, timing of energisation, degree of advance notification, ranking in scheduling conflicts, etc.

5.1.5 Similarly, the Subchapter 7.3 and 7.4 processes may need to deal differently with events occurring within an integrated mining network or connection point compliance facility (and in particular in the Pluto facility given its special treatment under the rules).

Issue 3: The definition of "notifiable event" is very broad. The Subchapter 7.3 and 7.4 processes may need to differentiate between, and integrate across, different classes of notifiable event, for example:

- **planned maintenance and routine upgrades;**
- **major or extended outages;**
- **commissioning and testing;**
- **events in integrated mining networks;**
- **events in the Pluto facility; and**
- **events in another connection point compliance facility.**

5.1.6 As a drafting matter, the ISO observes that the rules are not wholly consistent in how they refer to "planned outages" rather than "notifiable events". This should be tidied up in any rule changes which arise from this review.

[19] Rule 186(1), which deals with management of pre-contingent threats, does create some doubt about this conclusion because when dealing with the ISO's pre-contingent functions, it says "in order to preserve a secure state despite the external threat **or planned outage**" (emphasis added). This seems to imply that a planned outage could be a pre-contingent threat, which is inconsistent with the definition in rule 8. On balance, the ISO considers the emphasized words in rule 186(1) to be a mistake. The rest of the PNR presents (for better or worse) a fairly coherent whole, in which planned outages are contingencies and are not pre-contingent threats. In any rule changes which result from this review, the ISO will propose that this be tidied up.

5.2 “System coordination matters”

5.2.1 **“System coordination matter”** is also defined very broadly under rule 167, to include the scheduling and coordination of, and updates regarding, notifiable events, and also their likely impact on security, reliability and related matters, and their mitigation and management. This breadth is important because the machinery in Subchapter 7.3 and 7.4 applies in respect of these system coordination matters. If something falls outside this definition, then strictly speaking the processes in Subchapters 7.3 and 7.4 will not be activated.

5.2.2 The rules’ treatment of the *management and mitigation* of events is largely confined to including that subject as one limb[20] of this definition. This is discussed in section 6 below.

5.2.3 Otherwise, the ISO has not identified any particular issue with the definition of “system coordination matter”.

5.3 How planned outages fit into the definitions, and the resulting system state

5.3.1 The Rules contain two mechanisms to deal with anticipated operational events—the “notifiable events” regime in Subchapters 7.3 and 7.4, and the “pre-contingent threat” regime in rules 79(1)(d)(iv) (for the pre-contingent protocol) and 186 (for pre-contingent actions).

5.3.2 In managing recent planned outages, the ISO has discovered some shortcomings in the Rules’ drafting which have important operational implications.

The definitions

5.3.3 As noted, rule 166 gives **“notifiable event”** a broad functional definition, being basically anything planned or anticipated which might jeopardise system security. The definition gives examples which include an “outage”, which is defined in rule 8 to include any outage of “equipment”, the definition of which would include “network elements”.[21]

5.3.4 A planned outage is clearly a “notifiable event”.

5.3.5 Rule 8 defines **“contingency”** as including “… the … removal from operational service of one or more generating units or network elements, or the disconnection at a connection point of a registered facility”.

5.3.6 This definition does not specify or limit the *cause* of the removal or disconnection. Specifically, it does not exclude deliberate disconnections. Thus, a planned outage is almost certainly *also* a “contingency” on current drafting.

[20] Rule 167(c)(iii)

[21] See full definitions in the Appendix.

5.3.7 Finally, rule 8 also defines **"pre-contingent threat"**. This definition is closed, being "an approaching external threat … [an] impending material equipment failure, or … an imminent risk of physical injury … or … damage".

5.3.8 A planned outage does not easily fall into any of these categories. Although in some circumstances it is possible that a planned outage could involve an impending material equipment failure, this is not necessarily the case, so a planned outage will usually not constitute a "pre-contingent threat" on current drafting.

What is the system's operating state during a planned outage?

5.3.9 Subchapter 7.5 of the Rules envisages three operational states for the power system. These are:

(a) **"normal operating conditions"** – managed under rule 185;

(b) **"outside normal operating conditions"**, whether because of a contingency or otherwise – managed under rule 187; and

(c) **when there is a pre-contingent threat** – managed under rule 186.

5.3.10 The first two of these are mutually exclusive. The third is a special case which can co-exist with either of the others.

5.3.11 These defined states have important operational consequences. During normal operating conditions, power system management is in the hands of the NSPs – the ISO control desk has only a monitoring and administrative role, and no general power to issue directions. In the other two operating states, the ISO control desk (and perhaps other entities, if a protocol says so) has the power to activate a protocol and give directions, but only if the protocol's activation conditions are met.

5.3.12 It is the activated protocol, not the rules, which contains the ISO control desk's powers of direction. If a protocol cannot be activated, the ISO control desk is limited to monitoring and facilitation, as during the normal operating state.

Discussion

5.3.13 The ISO believes that the drafting of the rules in this respect does not align with the intended operational outcomes. Specifically, it considers that of the three operational states listed in paragraph 5.3.9, it may make more sense for planned outages to be managed in a manner more closely aligned to the regime for managing pre-contingent threats, than that for managing contingencies.

5.3.14 Like bushfires and cyclones, planned outages are a specific predictable event which likely requires non-BAU measures to be put in place before or during the event. In contrast, contingencies are generally managed reactively after the event has occurred. In those circumstances, the operational powers must be focussed on rapid response, which leaves less room to consider commercial matters or other users' operational convenience.

5.3.15 But as noted above, at present the rules' definitions produce the opposite result—under the current rules, a planned outage is a "contingency"[22] and therefore, during a planned outage the system will by definition always be outside normal operating conditions, because a contingency has occurred.[23]

5.3.16 The effect of this is that whenever a planned outage occurs, the rules as currently drafted expect the system to be managed under rule 187 (responsibility and powers following a contingency, etc) which is generally reactive management, rather than under rule 186 (pre-contingent actions) or rule 185 (normal operating conditions). This is not appropriate.

5.3.17 Depending on the frequency of planned outages across the system, this may mean that the system is not often deemed to be in a normal operating state.

Issue 4: Under the current rules, a planned outage is a contingency, and not a pre-contingent threat, and so falls to be managed under rule 187 which has a focus on reactive post-contingent responses.

Issue 5: Because a planned outage is a contingency, whenever a planned outage is occurring anywhere in the NWIS, the system is defined to be "outside normal operating conditions", enabling relevant protocols to be activated (if their activation conditions are met)—but the pre-contingent protocol will *not* be available. The ISO seeks stakeholder feedback on whether this is a desirable outcome, or whether:

(a) planned outages would be better managed as a variety of pre-contingent threat; or

(b) the definition of "normal operating state" should be changed so that the system can (or can sometimes) remain in this state despite planned outages being under way; or

(c) a fourth operating state is required, specifically to deal with planned outages.

5.3.18 Subject to stakeholder feedback, in the interests of simplicity, the ISO is inclined to avoid creating a fourth operating state. Rather, it suggests that the best approach may be to amend the rules and protocols so that planned outages can be managed as a special class of pre-contingent threat. A special class will likely be needed because notifiable events such as planned outages will typically allow longer preparation times, will come in more diverse forms, and can often last longer, than events such as bushfires and cyclones. And as noted in section 5.1 above, different classes of notifiable event may well need different treatment (e.g. planned maintenance versus testing and commissioning)

5.3.19 As a separate matter beyond the scope of this review, depending on where the rules land in terms of whether a planned outage or other notifiable event is or is not a contingency, the provisions of the *Pilbara Harmonised Technical Rules* may need to be reviewed, for example regarding frequency tolerances during single and multiple contingencies.

5.4 Notification of notifiable events

5.4.1 As noted above, under the rules a "notifiable event" as defined in rule 166 (which includes a planned outage) is a "system coordination matter" under rule 167.

[22] Rule 8 defines a "contingency" as an event affecting the power system involving the failure or removal from operational service of one or more generating units or network elements, or the disconnection at a connection point of a registered facility.

[23] Rule 165(a)

5.4.2 The primary method for notifying system coordination matters is at the fortnightly system coordination meetings,[24] although the rules also provide for the ISO to liaise with registered NSPs and ESS providers between meetings.[25]

5.4.3 Although this communication mechanism for notifiable events—discussion at the system coordination meetings and informal notification between meetings—reduces the administrative burden, it is not always desirable. For example many planned outages are known months or even years in advance, allowing ample time for orderly correspondence, modelling, and the like, thus reducing risk.

5.4.4 An ability to get early approval can also provide certainty to participants - i.e. certainty that maintenance can be scheduled (with specialist teams brought sometimes from around the world) or that a battery can commissioned and energised.

Issue 6: The rules rely primarily on oral discussion as the means for NSPs to notify the ISO and other NSPs of notifiable events. This minimises the compliance burden for near-term coordination, but may not be the optimum way to manage scheduling and assessment (including modelling) for outages which are known well in advance.

5.4.5 The rules do not specify the level of detail that needs to be included in a notification, referring only to the emphasis on communication and collaboration between the ISO and the registered NSPs regarding system coordination matters.[26] Nor do the rules provide for there to be a Procedure for outage management.

5.4.6 The requirement for additional detail is presently contained in the *Interim EBAS Procedure*[27] clause 3.14.4 which requires a responsible NSP to outline the following for each notifiable event at a system coordination meeting:

(a) its likely consequences on security and reliability; and

(b) its likely consequences in terms of whether a constraint rule is or is likely to be violated; and

(c) any measures which may be necessary or desirable to have in place for managing the power system in order to achieve the system security objective during the event, including any changes in essential system services (**ESS**) procurement, configuration, enablement and dispatch; and

(d) if it is a planned outage – whether it should proceed.

5.4.7 As noted above, other regimes have found it necessary to evolve much more detailed and intrusive regimes for outage notification and management. The ISO does not believe that the NWIS presently needs a regime of similar complexity, but does consider that the rules should allow the outage management regime to evolve as the NWIS evolves.

[24] rule 174(2)

[25] rule 175. Rule 179 requires reasonable steps to a GEIP standard to promptly notify any notifiable event that has not previously been notified and is likely to occur before the next system coordination meeting, or where there is a material change in circumstances to those previously notified.

[26] Defined in Rule 162.

[27] Interim Energy Balancing and Settlement Procedure available on the ISO's website.

5.4.8 For example, a System Coordination Procedure could the provide a mechanism (perhaps still the system coordination meetings) to triage notifiable events in terms of risks and consequences, and could specify a more thorough process for more serious events. It could allow for different processes and timing for different types of notifiable events. For example, the ISO could undertake the assessment and present it to the group using a standardised ISO risk framework.

5.4.9 A common Procedure and approach would overcome the present problem that NSPs are not in a position to model the impact of notifiable events beyond the bounds of their own network, and that different NSPs have different views on what is and is not a credible contingency.

5.4.10 This expanded role for the ISO would have resourcing implications. It would also need a means to resolve disagreements or disputes, including accountability for the ISO.

Issue 7: There is no Procedure regarding outage management and the rules do not provide for one.

5.4.11 The rules are prescriptive about the composition, agenda and duration of system coordination meetings. The ISO considers these rules to be too restrictive to allow sometimes complex outage planning matters to be discussed. They do not recognise the need to sometimes have different skill sets or resources included in the process, and do not allow the time sometimes required to resolve the risk and technical issues involved.

Issue 8: The rules regarding the composition, agenda and duration of system coordination meetings are too prescriptive. These matters may be better located in a Procedure.

5.5 Assessment of notifiable events

5.5.1 The rules are largely silent on how notifiable events are to be assessed. There is no explicit requirement in the rules that a notifiable event's impact on security, reliability, constraints or ESS be assessed or reported, and no person is explicitly made responsible for this task. These are all merely defined to be "system coordination matters"[28] and so are to be "discussed" at system coordination meetings.[29]

5.5.2 The rules then jump from this "discussion" to the ISO's "system coordination reports" which are to report on current or anticipated system coordination matters (which includes, as defined, impacts on security, reliability, constraints and ESS). But the rules give no guidance on how the meeting's discussion is to get to (what are presumably) the outcomes set out in the ISO's report. Presumably, this responsibility falls collectively on that meeting's attendees. This lack of clear responsibility is risky.

5.5.3 Nor do the rules allocate responsibility or provide any mechanism for:

[28] Rule 167(c)

[29] Rule 174(2)

(a) any risk and other assessments, or any modelling, which might be required before or as a result of the discussion (for example assessments of which contingencies may or may not be credible during the outage, and how those contingencies might be addressed); or

(b) accommodating the fact that different NSPs and network users may have different risk appetites or make different risk assessments; or

(c) accommodating the fact that not all rules participants have the same skills, resources or time to manage or assess these matters; or

(d) resolving any disagreements about any of the above matters.

5.5.4 The ISO considers these to be material shortcomings in the current regime and intends to propose measures to address them in which the ISO is tasked as the final determiner of system coordination matters and the associated modelling and assessments.

Issue 9: The rules do not clearly allocate responsibility for determining the impacts a notifiable event might have on the power system, including security, reliability, constraints and ESS, or for the risk and other analysis and modelling required to assess these things, and do not provide a mechanism for accommodating different risk appetites or resolving disagreements on these matters.

5.5.5 In general, the ISO considers that the delegation of the ISO control desk function to Horizon Power is a matter for EPWA's EPNR review, rather than this review. But there is one area which relates directly to the Subchapter 7.3 and 7.4 processes.

5.5.6 At present, the ISO draws on advice and opinion from ISO control desk staff when assessing notifiable events, including risk assessment and how the event may be mitigated and managed. Where there is a difference of opinion between Horizon Power and other NSPs, this can create at least the perception of a conflict of interest. This places a focus on Horizon Power's measures to manage such conflicts.

Issue 10: If there is disagreement between Horizon Power and another NSP regarding the assessment of a notifiable event, the ISO's use of ISO control desk staff to help in the assessment places a focus on how Horizon Power manages the staff's conflict of interest.

5.6 Approval of notifiable events

5.6.1 The rules, by design, have no general requirement that outages or other notifiable events be approved before they may proceed.

5.6.2 Although this minimises the administrative load, it may become increasingly difficult to sustain as the NWIS becomes more dynamic. The key issue is how various notifiable events may interact with each other, which is likely to become increasingly complex as more solar and storage, and eventually wind, projects are tested and commissioned.

5.6.3 ISO is not presently resourced to act as a central register and approver of all notifiable events.

Issue 11: There is no general requirement for planned outages and other notifiable events to be approved.

5.6.4 At present, if the informal and collaborative processes identify a problem, there is no mechanism to resolve it. Unless there is a "scheduling conflict" (see section 5.7), the rules lack any power for the ISO to intervene to stop, defer or otherwise give directions regarding a planned outage, if questions regarding its impact on security, reliability, constraints and ESS remain unresolved. The ISO considers this a material shortcoming.

Issue 12: Except in the case of a scheduling conflict, the rules to not provide for a notifiable event to be stopped or deferred, or otherwise be the subject of a direction, pending satisfactory resolution of any disagreement regarding its impacts on other participants, e.g. by way of its impact on security, reliability, constraints or ESS.

5.7 Coordination of events and managing scheduling conflicts

5.7.1 Scheduling conflicts are to be resolved by consensus wherever possible.[30] This is desirable and should be retained.

5.7.2 This is the one instance in which the ISO can intervene to give a direction regarding a notifiable event.[31] However, the ISO considers some details of this power to be suboptimal.

5.7.3 Under the rules, a **"scheduling conflict"** arises for an outage if the ISO determines that the outage, taken together with all currently proposed or anticipated notifiable events, may cause the power system to be outside the technical envelope, or otherwise poses an unacceptable risk to security and reliability.[32]

5.7.4 The ISO considers this definition to be too narrow:

(a) As noted in section 5.6 above, it only assesses outages in combination with some other notifiable event. It does not allow outages to be considered in isolation.

(b) The main threshold for intervention is the system going outside the technical envelope. The ISO is thus not able to intervene for outages which would only take the system outside a secure state. This does not align with the system security objective (which targets the higher standard of secure state).

(c) The secondary threshold for intervention is limited to unacceptable risks to security or reliability. There is no consideration of other effects on system participants such as through the combined outages' effect on risk, constraints, ESS or costs.

5.7.5 The ISO can only intervene to give a direction if it has first determined that a consensus is unlikely to be reached in time.[33] While it is desirable to give priority to consensus resolution of scheduling conflicts, as a matter of administrative process this inserts an extra formal step the ISO must complete before it intervenes.

[30] Rule 182(2)

[31] The ability for the ISO to issue a "direction" excludes issuing a direction to the Pluto Facility's Controller and if the scheduling conflict involves both a covered network and an integrated mining system, the ISO is to have regard to Rule 5.

[32] Rule 182(1)

[33] Rule 182(3)

Issue 13: The definition of scheduling conflict is limited to events which may take the system outside the technical envelope or otherwise pose an unacceptable risk to security or reliability. This does not require the system to be maintained in a secure state, and does not assess other impacts such as on risk, constraints, ESS or cost.

Issue 14: The ISO's power to intervene in a scheduling conflict is not enlivened until it has first determined that a consensus is unlikely to be reached in time. This could create system risk.

Issue 15: Are the ISO's direction powers under rules 182(3) to (5) appropriate and sufficient?

5.7.6 As a drafting point, rule 182 is internally inconsistent. The test in rule 182(1) for when a scheduling conflict exists is whether the power system will move outside the technical envelope. But in rule 182(5), the ISO's directions power is framed in terms of the system security objective, which includes maintaining the power system in a secure state where practicable.[34] In any rule changes which result from this review, the ISO will propose that this be tidied up in favour of the higher standard.

[34] Rule 162(b)

6. Managing and mitigating notifiable events

6.1 The role of network planning criteria

6.1.1 **"Network planning criteria"** refers to the network's design philosophy, and in particular the levels of redundancy to be built into the network (N-0, N-1, N-2, etc). The Pilbara regime recognises that Pilbara networks operate within a unique set of geographical, load and environmental circumstances, and so the PHTR do not prescribe a single set of network planning criteria. Rather, they allow each NSP to determine and publish its own criteria.[35]

6.1.2 The rules then allow for the resolution of "planning criteria interactions" in which one NSP's criteria may adversely impact another network's security or reliability,[36] and allows for a protocol to deal with these matters.[37]

6.1.3 The rules allow the ISO to take network planning criteria interactions into account when performing functions under Chapter 8 (ESS and energy balancing and settlement).[38] There is no equivalent provision for the outage planning and assessment process under Subchapters 7.3 and 7.4.

6.1.4 This topic goes to risk assessment—what risk is acceptable during a planned outage or other notifiable event? For example, is it OK for part of the network to operate at N-0 during an outage simply because other parts of the network normally operate at N-0? Alternatively, if a part of the network normally operates at N-2 and an outage reduces this to N-1, when is it appropriate to incur the cost of mitigation measures to return the system to an N-2 standard?

Issue 16: The rules do not deal with how network planning criteria are to be dealt with in assessing, managing and mitigating notifiable events.

6.1.5 One specific and similar issue which has arisen in managing recent outages is that the rules currently treat islanding as a binary issue—either a portion of the network is in synchronous connection with the rest of the network, or it is not. In fact, as recent experience in connection with one long duration planned outage showed, outage management also needs to deal with situations in which the remaining interconnections may be weak.

6.1.6 For example, if a potential island remains synchronously interconnected but net imports to that potential island are capable of exceeding the thermal capacity of the remaining interconnector, then prudent system management may require pre-contingent actions, such as placing a constraint to be placed upon that interconnector, or starting a machine within the potential island to prevent the interconnector from being overloaded. Similarly, ESS activation may need to change, to ensure that there is adequate FCESS and SRESS available within the potential island should the actual islanding event occur.

6.1.7 Neither the current protocols nor the current ESS regime in Chapter 8 deal cleanly with this scenario.

[35] *Pilbara Harmonised Technical Rules*, rule 2.5

[36] Rule 72

[37] Rule 79(1)(d)(iii)

[38] Rule 246

6.1.8

Issue 17: The rules and protocols do not deal cleanly with a situation in which islanding has not yet occurred but pre-contingent actions are necessary, e.g. to prevent islanding or ensure the island is secure (or at least inside the technical envelope) should islanding occur.

6.2 Managing notifiable events and mitigating their effects

6.2.1 Whatever decision may be made as to how the system state is described during a planned outage or other notifiable event (see section 5.3 above), it's clear that managing and mitigating some outages may require non-BAU measures. For example, a line outage may mean that the risk of an islanding event increases, such that different ESS arrangements may be needed. Alternatively, a line outage may make it necessary to impose constraints on other lines which remain in operation. Equipment recall arrangements may be needed. For brevity this paper calls all such operational responses **"mitigation"** measures.

No obligation to implement mitigation measures

6.2.2 The Rules impliedly recognise the potential need for mitigation measures, by including them as one limb of what are to be discussed as "system coordination matters",[39] but beyond that the implementation of these measures is largely unregulated.

6.2.3 Except for scheduling conflicts, the ISO's powers in relation to these matters are limited to making recommendations in a system coordination report,[40] but there is no obligation on rules participants to comply with these recommendations.

6.2.4 As a result, the decision on such measures sits in the hands of the individual NSPs, but the rules do not currently place any specific obligation on rules participants to design or implement mitigation measures in respect of a planned outage. These matters are regulated only indirectly, through general obligations such as:

(a) rule 168(1) which requires system operations participants to perform functions to a GEIP standard;

(b) rule 185(1) which requires a registered NSP during normal operating conditions to operate and maintain its network with a view to achieving the system security objective and not to do anything or cause anyone else to do anything which might reasonably be expected to lead to the power system being outside the technical envelope (noting that this obligation only refers to the lower *technical envelope* threshold rather than the higher *secure state* threshold).[41]

6.2.5 At present this gap is being filled by clause 3.14 of the *Interim EBAS Procedure*, which states that the responsible NSP which has caused the notifiable event must have in place necessary arrangements that meet the system security objective. Although better than nothing, this does not recognise that

[39] System coordination matters under Rule 167(c)(iii) include "any measures ,… desirable to put in place for managing the Power System…to achieve the System Security Objective during the event …".

[40] Rule 177(1)(b) and (c)

[41] This is relevant because a failure to mitigate a planned outage may only take the system outside a secure state and not outside the technical envelope.

sometimes the mitigation of an outage may require action by someone other than the responsible NSP. It is also not optimum to have this general outage-management obligation recorded in a procedure which is primarily directed towards EBAS matters.

Issue 18: There is no clear mechanism for identifying the measures necessary to manage or mitigate a notifiable event, and no clear obligation on any person to implement those measures once identified.

No mechanism to resolve disagreements

6.2.6 There is also no practical mechanism to resolve differences of opinion as to how outages should be managed or mitigated, and what level of risk exists or is tolerable during the proposed outage. (In theory a participant could commence a rules dispute, but this would be too slow to be useful, and would be a cumbersome and excessive mechanism.)

6.2.7 Experience has shown that participants can become deadlocked on matters of risk assessment.

Issue 19: There is no practicable mechanism to resolve differences of opinion in connection with notifiable events, for example regarding risk assessment and how or by whom a notifiable event is to be mitigated or managed.

What operational standards should apply during a notifiable event?

6.2.8 On one occasion, a rules participant suggested that the ISO may exempt it from the system security objective during a notifiable event, on the basis that compliance with that objective was too burdensome or expensive.

6.2.9 It is true that the overall level of system risk may sometimes be higher during a notifiable event. On some occasions, the cost of completely mitigating this risk may not be justified.

6.2.10 However, the system security objective lies at the heart of the Pilbara regime and should not lightly be set aside. At present, the ISO is inclined to the view that provided the regime to determine mitigation measures and responsibilities is adequate, and the costs of those measures are apportioned appropriately, there should be no need to dilute rules participants' obligations regarding system security.

Issue 20: A question has been raised as to whether there should be any exemption from rules participants' system security obligations during a notifiable event.

No integration with the ESS regime

6.2.11 Experience has shown that the question of how to mitigate the risks of a planned outage or other notifiable event can overlap significantly with the question of how much ESS the ISO should procure, and of what type. Indeed clause 3.14.7 of the *Interim EBAS Procedure* explicitly contemplates that ESS may be one of the mitigation measures.

6.2.12 The ISO considers that the rules may need to deal separately with the questions of the specification and procurement of, and cost recovery for:

(a) ESS for normal system operations; versus

(b) machine start services and other services (possibly including additional ESS) to mitigate planned outages and other notifiable events.

6.2.13 For the latter, the planned trial of Secondary SRESS may provide an operational solution, but it remains to be determined whether that mechanism on its own will produce the correct cost allocation outcomes (see section 6.3 below).

6.2.14 It may be that some or all of the rules can be common across these two streams, but that remains to be determined.

Issue 21: The rules do not deal separately with the specification and procurement of, and cost recovery for, additional ESS, or machine start or other services, when this is required to manage or mitigate a notifiable event, rather than as part of normal system operations under Chapter 8.

6.2.15 On the subject of ESS, the ISO raises three matters of detail:

(a) The language used to discuss ESS specification, procurement and cost recovery in each of the two streams listed in paragraph 6.2.8 may need to be fine-tuned, depending on how the issues discussed in section 5.3 are resolved—that is, whether during a notifiable event the system is considered to be in a normal operating state or some other state (non-normal, pre-contingent or some fourth state).

(b) Related, the language of rule 214(2)(b) sits uncomfortably with the dichotomy described in paragraph 6.2.8. On one reading, that rule could be seen as obliging the ISO to procure SRESS (e.g. Secondary SRESS) and recover its costs through the mechanisms in Subchapter 8.3, whenever this might be occasioned by a notifiable event, although the mechanisms for determining Required Headroom or Required Headroom Level would not seem to work properly in such instances. This should be tidied up as part of any changes to address the mitigation issues discussed in this section 6.2 and the cost-recovery issues discussed in section 6.3 below.

(c) The interactions between the currently on-trial Secondary SRESS and mitigation of notifiable events needs to be clarified. It may be that the service itself is an appropriate mitigation tool, but that the cost recovery mechanisms need to be different when it is used to mitigate certain types of notifiable event such as planned outages.

Limited powers for ISO to intervene

6.2.16 As noted, except for incomplete powers[42] in relation to scheduling conflicts, the ISO's powers in relation to the management and mitigation of notifiable events are mostly limited to making non-binding recommendations in a system coordination report.[43] This is unsatisfactory.

6.2.17 The types of intervention required to properly manage notifiable events will likely be of a different nature, and emerge on different timescales, than the interventions required to deal with contingencies. The latter presently reside with the ISO control desk under protocols. The former may sit better with the ISO itself, especially while the ISO control desk function is delegated to one of the

[42] See section 5.7 above

[43] Rule 177(1)(b) and (c)

NSPs. The timing is very different—post-contingent responses likely occur in minutes or hours, whereas interventions to manage notifiable events will likely occur months or weeks in advance (although control desks will still liaise in real time to manage the event).

6.2.18 Assuming the ISO is to be given powers to manage these matters, they could be housed in a form of pre-contingent protocol, in a System Coordination Procedure, in the rules, or some combination of these.

Issue 22: The ISO has no power to direct how a notifiable event is to be managed or mitigated.

Issue 23: The nature and timing of pre-contingent powers required to manage notifiable events are likely sufficiently different to the post-contingent powers the ISO control desk needs to manage contingencies, that it is appropriate for them to be exercised by the ISO rather than the ISO control desk. The current pre-contingent protocol was not designed to manage notifiable events.

6.2.19 The current *Protocol Framework Procedure* will need some adjustment to integrate the management of notifiable events. In the process, the ISO has identified some areas of the current protocols which should be tidied up, including:

(a) There is some doubt as to which of the protocols in the *Interim Protocol Framework Procedure* would be available to assist in managing the effects of a notifiable event, and a planned outage in particular. Protocols A1 and A3 activation conditions are limited to "unplanned" losses of network elements or generation or load respectively. On a conservative reading, Protocol B activation conditions may be limited to *only* "non-credible … or multiple contingency events" which will usually not catch a single planned outage. Protocol C is limited to pre-contingent threats which as discussed above may not include planned outages.

(b) As a result, there is some uncertainty as to whether and in what circumstances the ISO or the ISO control desk can activate a protocol to enliven a power to issue directions to deal with a planned outage. It's possible that this power may not be available until after something else goes wrong (i.e. another contingency occurs).

(c) Also, assuming Protocol B (the "catch all" protocol) applies to notifiable events, this protocol arguably cannot be activated until after the relevant contingency has caused the power system to be outside the technical envelope—thus arguably precluding preventative actions, and also precluding interventions if the system is in an insecure state but so far managing to remain inside the technical envelope.

6.3 Costs of mitigating planned outages and other notifiable events

6.3.1 A related but distinct consideration is who should pay for any necessary mitigation measures. The rules are currently silent on this point.

6.3.2 The *Interim EBAS Procedure* partially fills this gap by providing at clause 3.14.7 that the responsible NSP (being the NSP who has caused the notifiable event) is to contract and pay for additional essential system services required to ensure the notifiable event is managed in accordance with the system security objective. This measure needs expansion and further consideration.

6.3.3 It needs *expansion* because it does not recognise that management and mitigation of a planned outage or other notifiable event may require measures other than ESS.

6.3.4 It needs *further consideration* because although a 'causer pays' approach has some intuitive appeal, it may not always produce the best outcomes.

6.3.5 For example, a causer pays approach can create a perverse incentive against scheduling outages (although this in turn will be mitigated by the NSP's general obligation to maintain its network with a view to achieving the system security objective[44]). A causer pays approach also may not adequately recognise that many planned outages produce system-wide benefits, or at least can benefit users more broadly than just those in the particular network.

6.3.6 To address this, a 'beneficiary pays' model, while more complex, may be more appropriate. The crudest version of a beneficiary pays system would provide that all such costs are to be socialised across all system participants, on the simplistic basis that everyone benefits directly or indirectly to some extent from a properly maintained system.

6.3.7 Of course, moving away from a causer pays model can also have perverse outcomes, because it removes the incentive for the responsible NSP to undertake the outage in a way which minimises mitigation costs.

6.3.8 Then for each specific outage, there must be a clear process to identify which mitigation actions are properly counted as costs of the planned outage, and which should be classified in some other way.

6.3.9 Where the mitigation action involves a machine start, the determination of the resulting cost may be relatively non-controversial. But the rules will also need to provide a way to determine a fair cost for other mitigation measures such as network constraints.

6.3.10 Finally, any model which seeks to impose costs upon a person which that person does not themselves incur, will need a mechanism to ensure that the costs being passed on are prudent and efficient.

6.3.11 In some limited instances, there may already be a cost recovery mechanism. For example, if the ISO chose (and was permitted) to procure additional ESS (e.g. Supplementary SRESS) to mitigate the risks of a planned outage or other notifiable event, then (absent any rule changes) those costs would be recovered under the existing cost allocation mechanisms in Chapter 8. Whether this produced a fair outcome or the correct incentives, is another matter.

6.3.12 The ISO suggests that all of these deficiencies need to be addressed.

Issue 24: The rules lack any mechanism to determine and apportion the costs of managing and mitigating notifiable events. A choice needs to be made as to whether mitigation costs should be apportioned on a causer pays, beneficiary pays or socialised basis, or some combination of these or some other basis.

[44] Rule 185(1)

7. Other matters

7.1 Transparency and accountability on system coordination matters

7.1.1 The focus on communication and collaboration in respect of system coordination matters in the rules is indicative of the foundational regulatory regime. Subchapters 7.3 and 7.4 contain protections in respect of confidential information exchanged in the course of meetings or discussions on system coordination matters.[45] These protections are designed to ensure confidential information is not disclosed or accessible beyond the person's operational staff (with exceptions for audit, compliance and governance purposes) and not used, stored, analysed or disseminated for any purpose other than the purposes of Subchapters 7.3 or 7.4, or otherwise to achieve the system security objective.

7.1.2 However, the regime should have a bias towards transparency except where there is a clear risk of genuine commercial harm or anti-competitive outcomes.

7.1.3 Transparency will also be important in ensuring that the ISO remains efficient and accountable in exercising any of the broader functions contemplated above.

Issue 25: The regime for notifying, assessing, managing and mitigating notifiable events must appropriately balance transparency, accountability, confidentiality and competition.

7.2 Resourcing

7.2.1 Many of the solutions to the issues identified in this paper would involve a greater role for the ISO. This would have resourcing implications, which would likely impact on the ISO's fees.

Issue 26: If the ISO is given an expanded role to address the issues identified in this paper, it would have resourcing and hence cost implications.

[45] rule 176

Attachment 1: Relevant Rules

Subchapter 1.2 - Interpretation

…

8 Glossary

(1) A word or phrase defined below has the meaning given —

…

Contingency {also **Contingency Event**}: Means an event affecting the Power System involving the failure or removal from operational service of one or more Generating Units or Network Elements, or the disconnection at a Connection Point of a Registered Facility.

…

Pre-Contingent Threat: Means —

a) a Credible imminent threat to the System Security Objective arising from —

i) an approaching external threat (such as a storm or bushfire); or

ii) impending material Equipment failure,

or

b) an imminent risk of physical injury or death to any person or material damage to Equipment,

which can be mitigated if appropriate preparatory measures (Pre-Contingent Actions) are taken.

…

Subchapter 7.1 – Key concepts

162 The System Security Objective

The **"System Security Objective"** is to —

(a) Maintain the Power System Inside the Technical Envelope where practicable, and otherwise Promptly return it to Inside the Technical Envelope; and

(b) Maintain the Power System in a Secure State where practicable, and otherwise return it to a Secure State as soon as practicable; and

(c) otherwise — to a GEIP standard Maintain, and to a GEIP standard seek to improve, Security and Reliability.

163 Definition of Inside the Technical Envelope

(1) The Power System is operating **"Inside the Technical Envelope"** whenever all of the following conditions are satisfied —

(a) the frequency at all energised busbars is within the Frequency Operating Standards set out in the Harmonised Technical Rules; and

(b) the voltage magnitudes are within the normal range set out in the Harmonised Technical Rules at all energised busbars in a switchyard or substation at a Generation Facility, or on a Transmission Network or Interconnector; and

(c) the MVA flows on all registered facilities and Network Elements are within the applicable Operating Ratings and Security Limits; and

(d) the Power System is configured such that the severity of any potential fault is within the capability of the relevant circuit breakers to disconnect the faulted circuit or Equipment.

(2) The Power System is operating **"Outside the Technical Envelope"** whenever any of the conditions listed in rule 163(1) is not satisfied.

164 Definition of Secure State

The Power System is in a **"Secure State"** if it is —

(a) operating Inside the Technical Envelope; and

(b) subject to rule 72(4), expected to remain Inside the Technical Envelope following the occurrence of a single Credible Contingency event.

165 Definition of Normal Operating Conditions

A Power System is under **"Normal Operating Conditions"** when —

(a) no Contingency has occurred; and

(b) no Islands have formed; and

(c) no System Operations Direction is in effect; and

(d) frequency is within the Normal Frequency Tolerance Band; and

(e) the Primary FCESS Provider is providing the Primary FCESS service in accordance with the Primary FCESS Contract; and

(f) each contracted SRESS Provider is maintaining the amount of Headroom required by its SRESS Contract; and

(g) electricity flows across Interconnectors are within the tolerances agreed by the Interconnected NSPs and notified to the ISO; and

(h) no Pre-Contingent Actions are being taken.

166 Definition of Notifiable Event

A **"Notifiable Event"** for a Power System is any planned or anticipated system event (including a planned Outage, commissioning or testing of a Facility or Network Element) which might credibly be expected to adversely affect —

(a) Security or Reliability; or

(b) the ability of any part of a Covered Transmission Network to benefit from Essential System Services; or

(c) the ability of a Covered NSP to provide Transmission Voltage contracted Network services.

167 Definition of System Coordination Matters

The following are **"System Coordination Matters"** —

(a) the scheduling and coordination of all planned or anticipated Notifiable Events; and

(b) any changed circumstances or material new information regarding any planned or anticipated Notifiable Event; and

(c) for each currently planned or anticipated Notifiable Event —

(i) its likely consequences for Security and Reliability; and

(ii) its likely consequences in terms of whether a Constraint Rule is, or is likely, to be violated; and

(iii) any measures, which may be necessary or desirable to put in place for managing the Power System in order to achieve the System Security Objective during the event, including any changes in Essential System Service procurement, configuration, Enablement or Dispatch; and

(iv) if it is a planned Outage — whether the Outage should proceed as planned or at all;

and

(d) any other matters affecting Security, Reliability or system operations generally which are appropriate for discussion under Subchapter 7.3.

Subchapter 7.3 – System coordination

173 Objectives of this Subchapter 7.3 and Subchapter 7.4

(1) The primary objective of this Subchapter 7.3 and Subchapter 7.4 is to —

(a) promote communication and collaboration between the ISO and Registered NSPs regarding System Coordination Matters; and

(b) in so doing provide the ISO, Registered NSPs and ESS Providers with the information they reasonably need to perform their obligations under these Rules and relevant contracts, with a view to achieving the System Security Objective; and

(c) promote the collaborative resolution of Scheduling Conflicts regarding Outages and other System Coordination Matters; and

(2) The secondary objectives of this Subchapter 7.3 and Subchapter 7.4 is to do the above things in as efficient and informal a manner as practicable, maximising communication while minimising the compliance burden.

174 System coordination meetings

(1) The ISO is to convene a system coordination meeting at least once every fortnight.

(2) The system coordination meeting is to discuss, as necessary, any or all current and anticipated System Coordination Matters.

(3) A system coordination meeting is to be attended by —

(a) from each Registered NSP, a manager who has Direct operational responsibility for the personnel of an NSP who are engaged in system operations activities, or the manager's alternate; and

(b) an ISO representative, who is to chair the meeting.

(4) Unless the chair determines otherwise after consulting the Registered NSP representatives —

(a) the system coordination meeting's duration should normally not exceed 30 minutes; and

(b) a person identified in rule 174(3) may appoint an alternate from time to time; and

(c) the chair may permit one further ISO or Registered NSP representative to attend the meeting, to provide secretarial support; and

(d) otherwise, no-one else may attend a system coordination meeting.

{The intention is that meetings will predominantly involve the 4 people identified, and no-one else. The chair may from time to time invite others to attend, for example representatives from an ESS Provider or a major Load, but this is not intended to be a regular occurrence.}

(5) The ISO and Registered NSPs may agree on arrangements for system coordination meetings which differ from this rule 174.

175 Activities between system coordination meetings

Between system coordination meetings, the ISO will liaise as necessary with Registered NSPs and ESS Providers regarding System Coordination Matters.

176 System coordination meetings and discussions – Confidential Information

(1) A person who participates in a meeting or discussion under this Subchapter 7.3 or Subchapter 7.4 must —

(a) ensure that any Confidential Information it obtains in the course of the meeting or discussion is not disclosed or accessible beyond the person's operational staff (except to the extent reasonably necessary for audit, compliance and governance purposes); and

(b) not use, store, analyse or disseminate any Confidential Information it obtains in the course of the meeting or discussion, for any purpose other than the purposes of this Subchapter 7.3 or Subchapter 7.4 or otherwise seeking to achieve the System Security Objective.

(2) Rule 176(1) does not limit Subchapter 11.2 { Confidential Information}.

177 ISO to produce System Coordination Report

(1) After each system coordination meeting, and otherwise as it considers necessary, the ISO must give to the Registered NSPs and ESS Providers a report on —

(a) any current or anticipated System Coordination Matters; and

(b) any follow-up actions the ISO considers appropriate, including further discussions and the provision of further information; and

(c) any other thing the ISO recommends be done or not done, in respect of any of those matters.

(2) The format and content of the System Coordination Report is to be determined by the ISO from time to time in consultation with the Registered NSPs, placing an emphasis on meeting the objectives in rule 173 as simply and efficiently as practicable.

(3) The System Coordination Report is to be based upon information received by the ISO —

(a) at system coordination meetings;

(b) from Registered NSPs' internal Outage planning reports provided under rule 180(2)(b);

(c) otherwise from Registered NSPs.

(4) The ISO may inform itself as it sees fit in Connection with this Subchapter 7.3 and Subchapter 7.4, but does not have a general obligation to investigate planned or anticipated Notifiable Events beyond the information sources set out in rule 177(3).

178 Review of this Subchapter 7.3 and Subchapter 7.4

(1) From time to time, and at least once in every five year period starting from the Rules Commencement Date, the ISO must conduct a review of the processes set out in this Subchapter 7.3 and Subchapter 7.4 against the Pilbara Electricity Objective.

(2) The review must include consultation with Registered NSPs and registered controllers and Public consultation following the Expedited Consultation Process.

(3) At the conclusion of a review, the ISO must Publish a report containing any recommended changes to this Subchapter 7.3 or Subchapter 7.4.

(4) If the ISO recommends any Rules or Procedure changes in the report, it must either submit a Rule Change Proposal or initiate a Procedure Change Process, as the case may be.

Subchapter 7.4 – Notifying planned and unplanned Outages

179 If a near-term event arises between system coordination meetings

(1) If a Registered NSP, the ISO or the ISO Control Desk becomes aware of a pending Notifiable Event which has not previously been notified and is likely to occur before the next system coordination meeting, then (without limiting rule 183) it must take reasonable steps to a GEIP standard Promptly to notify, and coordinate with, as the case may be, the other Registered NSPs and the ISO Control Desk regarding the Notifiable Event.

(2) Rule 179(1) applies also to a previously-notified Notifiable Event if there is a material change from the circumstances as previously notified.

180 Notification obligations

(1) Each Registered NSP must notify the ISO and the other Registered NSPs of each planned or anticipated Notifiable Event on its Network, and must (to an extent which is reasonable having regard to the objectives in rule 173) keep them updated as information about the Notifiable Event changes.

(2) Subject to rule 179, a Registered NSP will be deemed to have complied with its obligation under rule 180(1) if it —

(a) provides the information orally at the next system coordination meeting;

{There is no minimum advance warning period for planned Outages. However, the effect of rule 180(2)(a) is to oblige the Registered NSP to raise a planned Outage at the system coordination meeting as soon as it appears on the Registered NSP's own planning horizon.}

and

(b) Promptly gives the ISO a copy of the Registered NSP's internal Outage planning report each time the internal report is materially updated.

(3) A Registered NSP may redact commercially sensitive information from a report given to the ISO under rule 180(2)(b).

181 Outages of facilities

(1) Each Registered NSP must ensure that it is kept sufficiently informed about Notifiable Events affecting facilities Connected to its Network, to Enable it to comply with its obligations under Subchapter 7.3 and this Subchapter 7.4.

(2) If a Registered Facility is Connected to a Covered Network, then the Registered Controller must keep the Covered NSP sufficiently informed about Notifiable Events affecting the Registered Facility, to Enable Registered NSPs and the ISO to comply with their obligations under Subchapter 7.3 and this Subchapter 7.4.

182 Resolving Scheduling Conflicts

(1) A **"Scheduling Conflict"** arises for a planned Outage if the ISO determines that the Outage taken together with all currently proposed or anticipated Notifiable Events, may cause the Power System to be Outside the Technical Envelope, or otherwise poses an unacceptable risk to Security and Reliability.

(2) Wherever possible, Scheduling Conflicts are to be resolved by consensus between the Registered NSPs, facilitated as necessary by the ISO.

(3) If the ISO determines that a consensus will not be reached in time for the relevant Notifiable Events to be managed appropriately, the ISO may resolve the Scheduling Conflict by giving a Direction to one or more of the affected parties but cannot give such a direction to the Pluto Facility's Controller.

(4) If the Scheduling Conflict involves, or involved facilities in, both a Covered Network and an integrated Mining System, the ISO must have regard to rule 5 in determining the content of a Direction under rule 182(3).

(5) A Direction under rule 182(3) may specify which Notifiable Event is to have priority for scheduling purposes, and may contain such scheduling or other information or instructions as the ISO considers reasonably necessary to resolve the Scheduling Conflict and achieve the System Security Objective.

183 Obligations to report contingencies and unplanned events

(1) The Registered NSP in whose Network a Notifiable Unplanned Event {defined in rule 183(5)} occurs, must Promptly on a 24/7 Basis notify the other Registered NSPs and the ISO Control Desk.

(2) An ESS Provider who suffers an unplanned Outage which will impact its ability to provide Essential System Services, must Promptly on a 24/7 Basis notify all Registered NSPs and the ISO Control Desk.

(3) A Generator who suffers an unplanned Outage of any Generating Unit which will or might credibly be a Notifiable Unplanned Event, must Promptly on a 24/7 Basis notify all Registered NSPs and the ISO Control Desk.

(4) The Protocol Framework is to set out communication requirements for notifications under this rule 183.

(5) In rule 183(1), an **“Notifiable Unplanned Event”** for a Network means any Contingency or other event, that might impact the Network in a way which might credibly be expected to adversely affect —

(a) achievement of the System Security Objective; or

(b) any part of a Covered Transmission Network’s ability to benefit from Essential System Services; or

(c) a Covered NSP’s ability to provide Transmission Voltage contracted Network services.