ElectraNet

1-05-OP01-P003

SECONDARY SYTEM DATA MANAGEMENT PROCEDURE

This procedure is in line with the organisation's Asset Management Policy

Reference the top level Organisational Policy from which this document operates.

Uncontrolled Copy

Document Control				
Approved By	Position	Senior Manager Network and Asset Management	Name	Michael Dobbin
Contact Position	Position	Network Engineer	Name	Armstrong Apollo
Contact Details	Apollo.armstrong@electranet.com.au			
Release Date	01/12/2014			
Date of Last Review	28/11/2018			

Revision Record					
Date	Ver.	Description Describe the nature of the changes	Author Name (Initial/Surname)	Checked By Name (Initial/Surname)	Approved By Name (Initial/Surname)
05/09/14	0.1	GHD Initial draft	J Gater	C Owens	G Jones
17/09/14	0.2	GHD draft	J Gater	C Owens	G Jones
24/10/14	0.3	GHD Final Draft	J Gater	C Owens	G Jones
17/11/14	A-1	ElectraNet Final Draft	J Gater	A Apollo	M Dobbin
28/11/18	B-1	Updated RSR Workflow Process	A Apollo	F Maio	M Dobbin

WHEN PRINTED THIS DOCUMENT IS UNCONTROLLED

COPYRIGHT AND DISCLAIMER

Copyright of this material is owned by or licensed to ElectraNet. Permission to publish, modify, commercialise or alter this material must be sought directly from ElectraNet. Reasonable endeavours have been used to ensure that the information contained in this document is accurate at the time of writing. However, ElectraNet gives no warranty and accepts no liability for any loss or damage incurred in reliance on this information.

CONTENTS

1. PURPOSE 3
2. SCOPE 3
3. TERMS AND ACRONYMS 3
4. PROCEDURE DETAILS 3
4.1 RELAY SETTING CHANGE 4
4.1.1 Creation of a System Change Notification (SCN) 5
4.1.2 Creation of a Global Setting Request (GSR) 5
4.1.3 Creation of Relay Setting Request (RSR) 5
4.1.4 Development and Authorisation 5
4.1.5 Apply and Validate 6
4.2 NOTIFICATIONS AND TIMING 8
5. PROCEDURE RESPONSIBILITIES 8
6. EVALUATION AND REVIEW 8
6.1 REVIEW 9
7. ASSOCIATED DOCUMENTS 9
7.1 RELEVANT LEGISLATION 9
7.2 POLICIES 9
7.3 GUIDELINES 9
7.4 PROCEDURES 9
7.5 FORMS 9
7.6 PROCESS MAPS 9
8. APPENDICES AND REFERENCES 9
APPENDIX A IPS-EPIS PROTECTION DATABASE ASSET VALUE CHAIN INTERACTION DIAGRAM 10
APPENDIX B IPS-EPIS INTEGRATION PROCESS 12
APPENDIX C IED CONFIGURATION CHANGE PROCESS 13
APPENDIX D RSR WORK FLOW PROCESS 14

Uncontrolled Copy

1. Purpose

Provide an explanation about the procedure and what the content intends to achieve.

This procedure describes how ElectraNet business groups, processes and procedures are required to interact with the IPS-EPIS Protection Database and the associated key activities and interfaces.

2. Scope

This section identifies to whom the procedure will apply and won't apply, what it covers and what it does not cover.

This procedure is applicable to all ElectraNet Business Groups personnel and contractors involved in any activity that interacts with the IPS-EPIS, be this engineering design, project management asset performance, commissioning, or operations and maintenance activities.

3. Terms and Acronyms

In the table below include a definition of a word or expression or limiting or extending the meaning of a word or expression that may be used in short form.

Term/Acronym	Definition
AMC	Asset Management Committee
Endorser	Responsible for nominating the group access level of endorsee. • Project Delivery – Project Manager • Engineering Field – Senior Engineer Protection • Network and Asset Performance Group – Principal Engineer Protection and Control • Asset Management Group – Network Engineer
EPIS	Enterprise Protection Information System The suite of IPS modules for protection relay management
GSR	Global Setting Request
IED	Intelligent Electronic Device
IEPD	IPS-EPIS Protection Database
NAP	Network and Asset Performance
RSR	Relay Setting Request
SCN	System Change Notification

Uncontrolled Copy

4. Procedure Details

This section must detail of the procedure in process order and may include links to other relevant documents, ie forms etc.

The Asset Management Value Chain Diagram provides a high level overview of interaction of the Business Groups and activities related associated with the IEPD through the Asset Lifecycle (see Appendices).

The process map 1-16-OP01-P018-PM002 IED Configuration Change Process (see Appendices) provides guidance though the interaction process. The steps contained in

the process map shall be followed to ensure correct and consistent interaction with the IEPD.

The key Business Groups and activities involved in the interaction are as follows:

Network and Asset Management: interaction management governance, monitoring, ongoing operation and maintenance and development of IEPD and related future IPS Asset Management and other software modules and programs.

Secondary Systems: Protection scheme and relay settings design including authorisation.

Project Delivery: Identifying operational protection issues and requirements and initiating and managing protection sub-projects within CAPEX and more significant OPEX Projects and Contractor Management and Network Operations roles.

Network and Asset Performance: Network asset issue and incident investigation, performance improvement requirements identification and initiating and authorising OPEX minor projects protection scheme and relay settings design and changes.

D&C and Maintenance Contractors: Design, implementation and testing and commissioning of Protection Schemes and Protection Relay Settings for CAPEX and OPEX projects under direction of Network Services.

4.1 Relay Setting Change

The IEPD provides a fully auditable settings change process and includes the following objects:

- System Change Notification. (SCN) The SCN represents any reason for a setting change. The SCN includes such data as:
  - Creating person
  - Assigned person or group
  - Name of Project or Maintenance Activity
  - Relevant documents if any, e.g. single line diagrams, wiring diagrams
  - SCN workflow definition

An SCN can include one or more Global Setting Request.

- Global Setting Request. (GSR) The GSR represents one or more relay setting request. A GSR includes such data as:
  - Workflow type
  - Target location or site
  - Assigned person or group
  - Setting creation instructions if any
  - GSR workflow definition

Typically all the relay settings changes required at a single site/substation would be recorded under one GSR. A GSR can include one or more RSR.

- Relay Setting Request. (RSR) The RSR represents one protection setting request for a single protection relay. The process is represented from the creation of date-setting, in-process calculations, to placing the new setting in active and in-service.

IPS-EPIS tracks the workflow and provides local alerts by email to inform relevant staff or external contractors of tasks to be completed. In addition all steps in the process are recorded in the IPS-EPIS database for quality assurance and review purposes.

Uncontrolled Copy

Different workflows can be setup within IEPD for different types of SCNs, GSRs and RSRs. These are setup within IEPD by the system administrator and can be updated as business requirements change.

The Setting Workflow Management module is described in section 17.1 of the User Manual.

4.1.1 Creation of a System Change Notification (SCN)

The requirement for an SCN is triggered by the identification of any protection setting change. Any authorised staff with access and initiates the cause to create new or alter relay settings should create the SCN.

In IEPD, the workflow for the SCN will lead to the creation of GSRs.

The SCN can only be closed once all the GSRs are closed.

4.1.2 Creation of a Global Setting Request (GSR)

The requirement for a GSR is triggered by the creation of an SCN. Only staff with authoriser access can create a GSR.

In IEPD, the GSR creator will assign the GSR to the required RSR implementers. A selection of users or groups is readily available. A local email in IPS will automatically sent to the nominated Setter, Comm. Supervisor, Commissioner, Setter Supervisor including the assigned Group or individual, once the GSR is completed.

The workflow for the GSR will lead to the requirement to develop one or multiple RSRs.

The GSR can only be closed once all relevant RSRs have been closed by the nominated approving authority.

4.1.3 Creation of Relay Setting Request (RSR)

An SCN and a GSR are required before an RSR is created. The RSR is the management tool for all Protection Relay setting changes and integration with IEPD.

This may be triggered amongst other by:

- Creation of a new network asset
- Configuration change to an existing network asset
- Change of network assets
- An identified correction of device settings

Regardless of the trigger, once it has been identified that a protection device is affected, a Relay Setting Request (RSR) must be raised in IEPD by the GSR and SCN creator by default. An RSR is presented in a Workflow Diagram in IEPD. The IPS-EPIS Integration Process Flowchart shows the interactions, tasks to be done and approvals for each step activity (see Appendices).

When a new RSR is created and assigned for development, a new set of “Provisory” Setting with status “Being Prepared” is added under the Relay Settings tab in IEPD. The Setting Developer could be from Network Services Group or from a third party contractor depending on the nature of the request. IEPD will automatically send a local email within the application to the nominated Setter, Comm. Supervisor and Commissioner containing the details of the request and actions to be undertaken.

See Section 17.1.3 – RSR Record in the User Manual for more detail on raising an RSR.

4.1.4 Development and Authorisation

Development of the solution should be in accordance with:

- 1-16-OP01-P018 IED Management Procedure

Uncontrolled Copy

Once the scope of the RSR has been created, the Setting Developer must upload the setting solution in IEPD. The authoriser will review the settings and if required, may request for another revision which will be recorded in IEPD. Each time a setting revision is uploaded, a new set of parameter setting revision in IPS should be created for it. The setting status will be updated from “Being Prepared” to “Applied for Approval” and date-setting shall be flagged as “Verified by” with the date and username of the setting developer confirming that a new set of setting revision is now forwarded for approval by the authoriser. Setting reports and other documents should also be attached under the “General” Tab in IPS while actual configuration files per revision should be attached under the “Relay Setting” Tab with reference to 1-16-OP01-P018-SD01.

Regardless of the trigger for the RSR, the Authoriser will always be an ElectraNet person with the relevant Authority, as described in procedure 1-16-OP01-P001.

The Authoriser will be advised via an email of the newly revised protection relay settings and will need to go to IPS to authorise the use of these protection relay settings. Once approved, the new setting should be flagged as “Issued by” with the date and user name of the Authoriser which confirms the developed setting is now ready for site implementation. At this stage, setting Status will be updated from “Applied for Approval” to “Ready for Operation”.

4.1.5 Apply and Validate

Once the new setting revision is approved, IEPD will notify via local email the nominated Setter and Commissioner responsible for application of the new protection relay settings. In most cases, these will be third party contractors.

Upon arrival on site, an “As-Found” comparison between the newly extracted relay settings from site against the current active setting in IEPD is required. Results of this comparison should be documented under the “Relay Setting Comparison” tab in the RSR. If the result of comparison failed beyond normal, the Setter should discontinue the workflow process and inform the authoriser about the significant comparison results. . An email will be sent back to the Authoriser to review settings comparison from site for the appropriate decision to continue.

When the result of as-found comparison is normal as expected, Setter and Commissioner will apply the New Settings in accordance with all applicable secondary commissioning management procedures and/or work instructions.

There may be times when the contractor is required to commission settings different to those that have been previously authorised/approved in IPS. In these instances, the contractor must follow 1-16-OP01-P018 IED Management Procedure.

Once the relay has been commissioned, the contractor must conduct another comparison between new relay settings and the previously authorised/approved setting in IEPD. This is known as the “As-Left” comparison and results should also be documented in the “Relay Setting Comparison” tab in the RSR. Results of the comparison should be “Pass”, if no new setting was introduced on site, otherwise “Fail”. Regardless whether pass or fail, the authoriser will review the results of the comparisons and decides accordingly to approved and continue with the workflow. Setting status in IEPD shall change to “Active” and “Applied for Approval” if comparison is “Fail” otherwise it shall be “Active” and “In-Service”. A new email will be sent to the Authoriser to verify and confirm the setting updates and comparison records.

In the unlikely event that a Design Error is found at this stage, a new set of RSR will be opened in IEPD and a new cycle of setting development to relay commissioning will take place. Otherwise, if everything is as expected, the Authoriser will also need to ensure that all other requirements have been complied with by the contractors. The authoriser then continues to “Seal” the settings in IEPD and update the setting Type from

Uncontrolled Copy

"Provisory" to "Proper" while previous active date-setting will be re-flagged as "Archived". An email with message RSR closed will be sent automatically to all user involved.

Uncontrolled Copy

4.2 Notifications and Timing

Whilst an automatic email notification was set up in IPS, it is still strongly encouraged that an external communication will be used as the main method of notification. This is to ensure that all required notifications amongst all parties are properly received as some companies and email servers treat and filter emails coming from an auto sending applications like IEPD as junk mails and/or fraudulent. The automatic notifications will now only serve as back up and/or redundant in the process.

Automatic notifications will be set up by personnel with Administrator rights, in accordance with section 9.6 of the User Manual.

IEPD will send automatic email notifications to the responsible person for each step of the process in accordance with RSR Workflow Definition in SWM Module of IPS-Energy.

Notifications can be sent from templates, or altered as necessary by the sender in order to ensure that the receiver has all the required information to allow them to complete their component/next step of the process.

There is a list of defined events that will trigger an email notification to be sent.

Staff must respond to all notifications internal or external emails. Timing of response is dependent on the actions required;

- Development – in line with design;
- Authorisations – within 2 business days;
- Testing Commissioning and Maintenance – in line with construction/commissioning program; and
- Verification – within 2 business days.

5. Procedure Responsibilities

This section details individual roles and responsibilities for the tasks mentioned within the document content.

Responsible Position	Responsibilities
Senior Manager Network and Asset Management	Owns, manages and approves the IPS-EPIS Protection Database Interaction Management procedure. Ensure Employees and other relevant Stakeholders have awareness of and comply with the procedure.
Network and Asset Management MS Administrator	Facilitate the review and publication of the procedure and verify user group requirements for new users.
Endorsers	Ensure that new users are appropriately trained in the use of IPS-EPIS according to their required level of access.
All Employees, Contractors, Consultants and Outsourced Providers	Comply with and act in accordance with the requirements of the procedure when creating, developing, authorising, applying or validating any activities within IPS-EPIS. Be familiar with the required sections of the IPS-EPIS User Manual.

6. Evaluation and Review

Evaluation: Include KPIs and detail how the procedure will be monitored to evaluate its effectiveness.

Uncontrolled Copy

Review: When and how often the policy is reviewed.

6.1 Review

This procedure will be reviewed every 2 years in accordance with 2-FR01-P001 Policy Development & Review Procedure.

7. Associated Documents

Include names and links to any relevant documents.

7.1 Relevant Legislation

None

7.2 Policies

1-02-OP10 Secondary Systems Design Protection and Automation Policy

7.3 Guidelines

None

7.4 Procedures

1-05-OP01-P001 Secondary System Data Configuration Governance and Administration

1-16-OP01-P018 IED Management

7.5 Forms

Not Applicable

7.6 Process Maps

1-16-OP01-P018-PM002 IED Configuration Change Process

8. Appendices and References

1-16-OP01-P018-SD01 IED Configuration Change Guideline

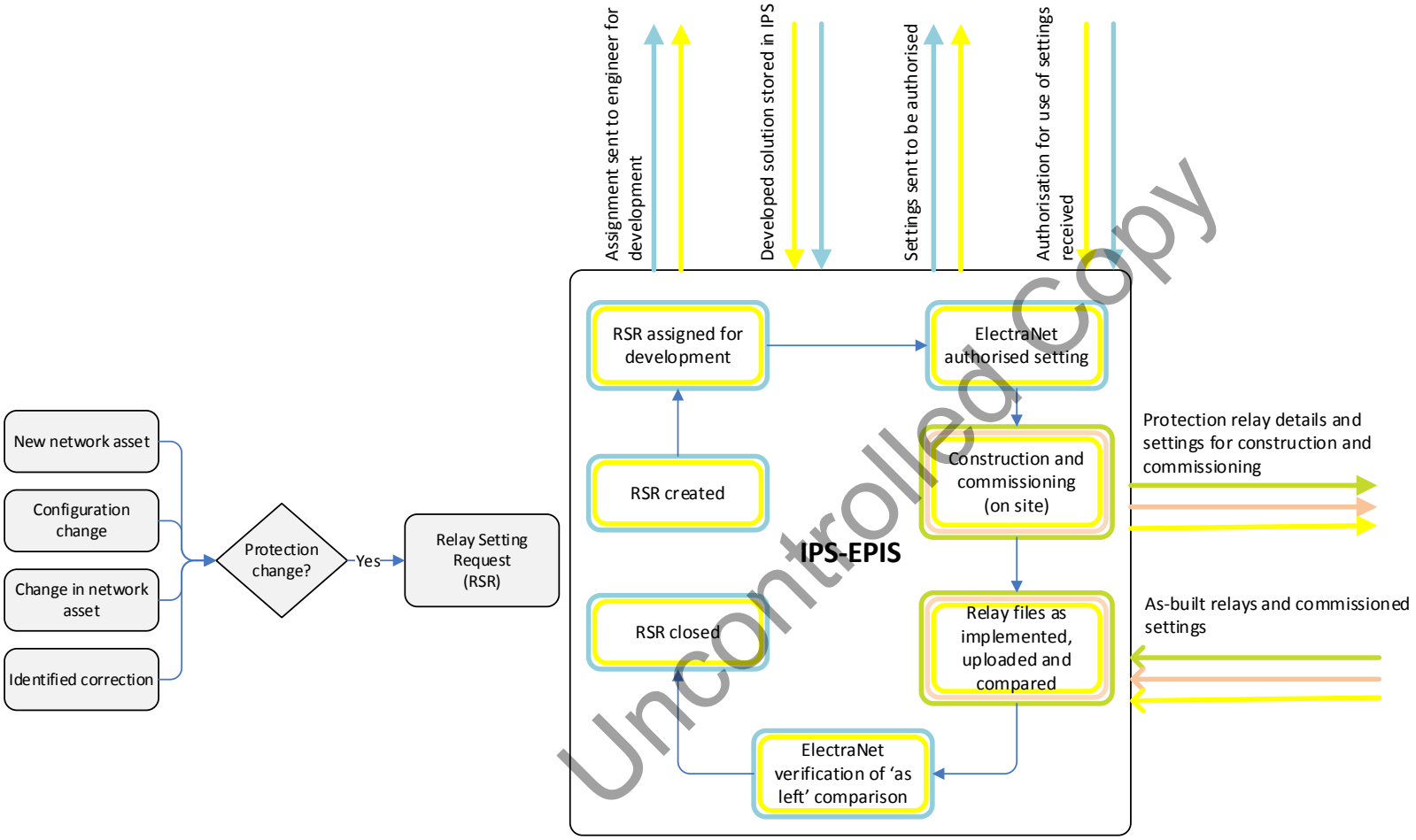
IPS-EPIS Protection Database User Manual 2010

Uncontrolled Copy

Appendix A IPS-EPIS Protection Database Asset Value Chain Interaction Diagram

ElectraNet Executive Management Level	Asset Management	Project Delivery						
Network Asset Value Chain	Strategy and Planning	Project Management	Design and Engineering		Construction and Commissioning		Operations and Maintenance	
ElectraNet Management Level	**Network and Asset Management** (Network and Asset Management strategy management decisions)	**Project Delivery** (Managing ElectraNet CAPEX and OPEX projects)	**Secondary Systems** (Provision of protection scheme and protection relay and setting designs)	**Project Delivery** (Manage contractor provision of protection relay and setting designs)	**Project Delivery** (Managing contractors for construction and commissioning activities)		**Network and Asset Performance** (Fault investigations, monitoring and improving network performance)	**Project Delivery** (Operating and maintaining the network, including management of contractors)
Organisation	**ElectraNet**	**ElectraNet**	**ElectraNet**	**Contractor**	**ElectraNet**	**Contractor**	**ElectraNet**	**Contractor**
Key IPS-EPIS activities	Develop and maintain Network Asset Value Chain and IPS-EPIS governance and QA policy and procedures.	Protection changes resulting from implementation of CAPEX and OPEX projects.	Producing and uploading the protection scheme and relay and setting designs into SPF-EPIS. Authorising protection relay and setting designs uploaded by contractors or Network and Asset Performance (if required) within IPS-EPIS.	Producing and uploading the protection scheme and relay and setting designs into IPS-EPIS for authorisation by Secondary Systems or Network and Asset Performance (if required).	Managing contractor to meet obligations outlined in the adjacent column.	Follow required procedures and obligations to extract protection relay and setting data from IPS-EPIS and achieve 100% compliance for uploading of accurate As-Built and commissioned protection relay and setting data into IPS-EPIS for verification by Secondary Systems or Network and Asset Performance (depending on project initiator).	Network and Asset Performance monitoring and fault investigation activities leading to requirements for corrective or improvement actions involving protection relay and setting changes. Temporary protection changes for operational reasons.	Follow required procedures and obligations to extract protection relay and setting data from IPS-EPIS and achieve 100% compliance for uploading of accurate changed protection relay and setting data into IPS-EPIS for verification by Secondary Systems or Network and Asset Performance (depending on project initiator)

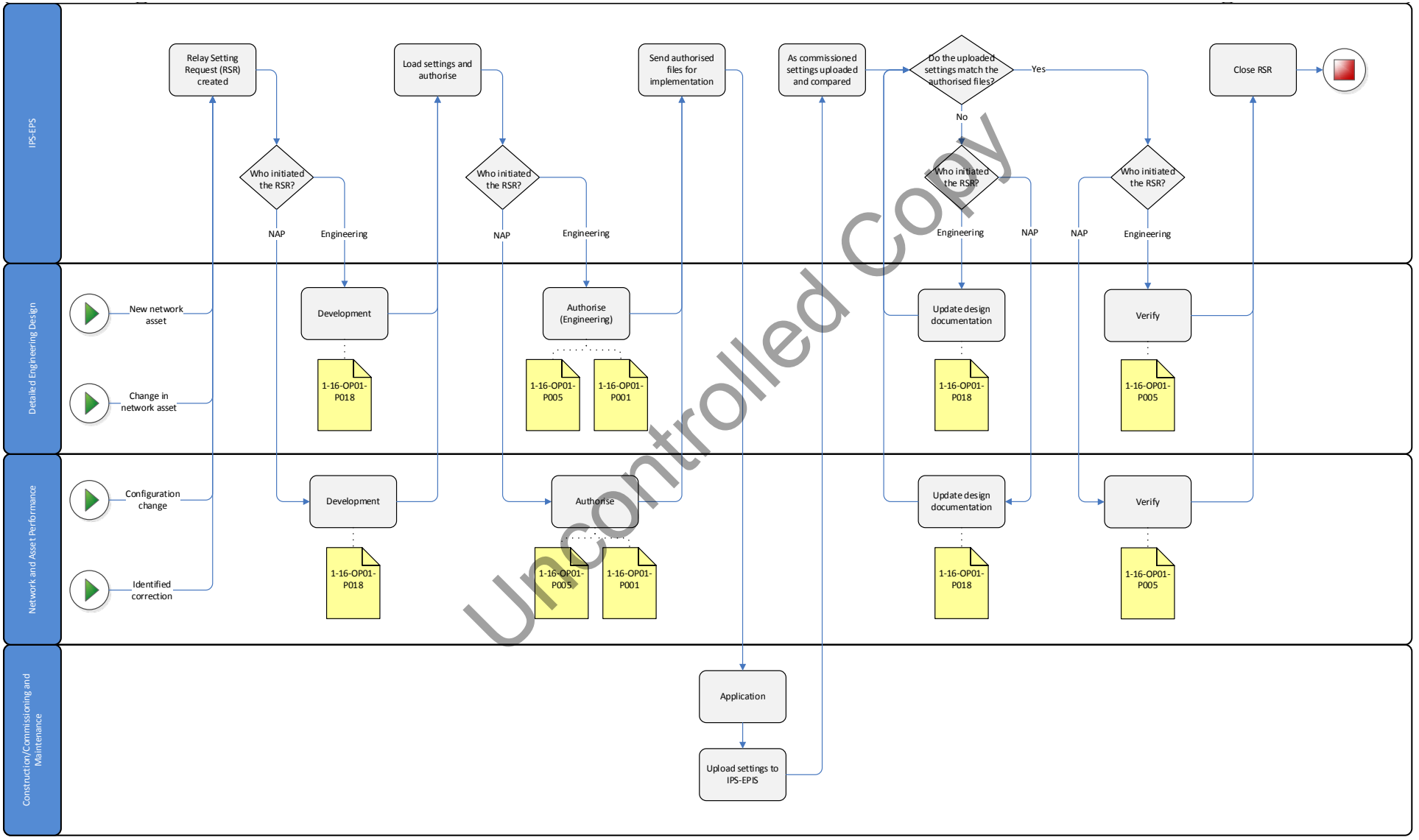
Uncontrolled Copy



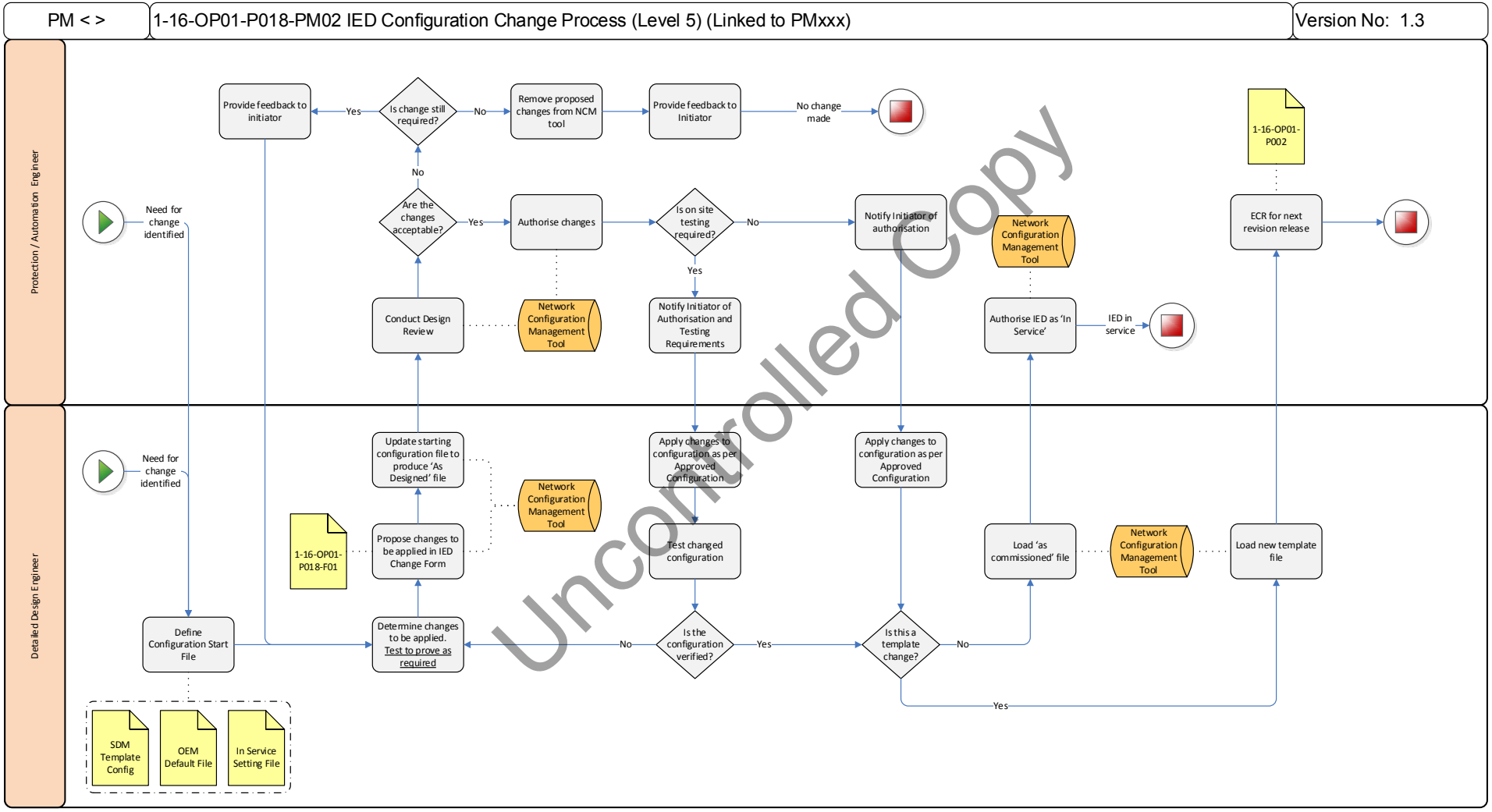
IPS-EPIS Database: Data Storage and Workflow Process Management

Uncontrolled Copy

Appendix B IPS-EPIS Integration Process

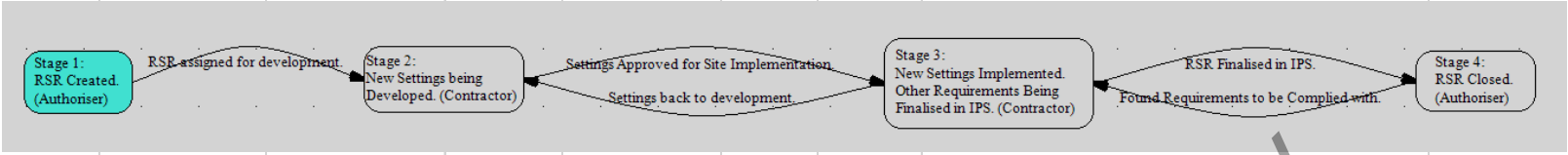


Appendix C IED Configuration Change Process



Uncontrolled Copy

Appendix D RSR Work Flow Process



WorkFlow Stage	WorkFlow Description	WorkFlow Movement	Setting Type	Setting Status	Setting Flag	Active Status	Work Flow Tasks	Responsibility
1	RSR Created	Initial Stage	Provisiory	Being Prepared			1. New RSR is created and assigned to contractor as required. 2. Notify contractor.	Authoriser
2	New Settings being Developed	**Contractor** need to move the workflow to this stage.	Provisiory	Applied for Approval	Verified by		1. Create New Setting Parameter. 2. Setting Parameter is renamed to indicate a new revision. 3. New set of setting parameters is uploaded in IPS. 4. Actual config file is attached and renamed to identify with the revision. 5. Notify Authoriser.	Contractor
			Provisiory	Ready For Operation	Verified by Issued by		1. Review and approve new setting revision. 2. RSR Data Tab ticked as "Ready for Site Implementation" 3. If setting does not meet approval, Setting Status and Flags should be reset to Workflow Stage 1. 4. Notify contractor.	Authoriser
			Provisiory	Ready For Operation	Verified by Issued by		1. Conduct "As-found" Comparison and record under "Relay Setting Comparison" Tab of the RSR. 2. If comparison "failed" contact Authoriser before proceeding. 3. If comparison "passed" proceed to update device. 4. Notify Authoriser.	Contractor
3	New Settings Implemented. Other Requirements Being Finalised in IPS.	**Contractor** need to move the workflow to this stage.	Provisiory	As-Left Comparison "Pass" - **In Service** "Fail" - **Applied for Approval**	Verified by Issued by	Ticked as **Active.**	1. Once the new setting is finalised and implemented on the device, an "As-Left" setting comparison should be recorder under the "Relay Setting Comparison" tab on the RSR. 2. Comparison should show "Pass" if no setting change is done on the approved setting for site implementation. Otherwise, a "Fail" will need to be further reviewed by the authoriser. 3. Finalised other requirements of RSR by ensuring the following : - Final Setting Parameter "As-Left" is uploaded as a new parameter set renamed as appropriate. - Final Setting config file including all other setting revision files are attached in "Relay Setting" Tab. - All setting reports and other documents should be attached under the "General" Tab. 4. Notify Authoriser.	Contractor
4	RSR Closed.	**Authoriser** need to move the workflow to this stage.	**Proper**	**In Service**	Verified by Issued by	Ticked as **Active.**	1. Review and approve the final applied setting. 2. Ensure that all other requirements in the RSR are complied with. 3. Close and Seal the RSR. 4. Archive the previous active Date-Setting. 5. Notify Contractor.	Authoriser

Uncontrolled Copy