Network Performance
Distribution System SCADA (DSS)
Capability Project

Project Note

Note Number	19
Title	Distribution System SCADA (DSS) Equipment and Systems - Forward Compatibility Requirements
Author	Neil Higgins
Version	0.6(a)
Release Date	
File Name	DSSForwardCompatibilityRequirementsForIEEE-DA-WG.doc

Amendment History			
Version	**Release Date**	**Author**	**Notes**
0.1		nah	First draft
0.2		nah	Review comments incorporated. Superfluous figures deleted. Observations on network awareness updated. Observations on close-onto-fault requirements added. Observations on decision making locale added. Forward compatibility requirements reformatted and updated.
0.3		nah	Observations on communications added. Observations on remote console access added. Precedence relationships added. Timeline added.
0.4		nah	Feedback incorporated. Forward compatibility requirements tidied up.
0.5		nah	Minor corrections.
0.6		nah	Words on embedded intra-system communications expanded. Words on IP enablement expanded. Third Order Systems section added. Words on forward compatibility requirements for SCADA communications expanded.
0.6(a)		nah	Copyright notice and disclaimer added for IEEE release.

1. Contents

1. CONTENTS 1

2. DISCLAIMER 3

3. PURPOSE 3

4. TERMINOLOGY 3

5. REFERENCED DOCUMENTS 3

6. DSA DEFINED 4

7. DIFFERENTIATING FEATURES 4
7.1 SCOPE AND OBJECTIVES 4
7.2 GRANULARITY 4
7.3 DECISION MAKING LOCALE 4
7.4 NETWORK AWARENESS 4
7.5 STANDARDS 5
7.6 IMPACTS 5
8. EXAMPLES 6
8.1 AUTOCHANGEOVER AND AUTORESTORATION 6
8.2 AUTOMATIC RECLOSING AND SECTIONALISING 8
8.3 S&C INTELLIRUPTER, SPEEDNET AND INTELLITEAM III 10
8.4 LOOP AUTOMATION 12
8.5 SP MANWEB URBAN AUTOMATION (UA) SYSTEM 14
8.6 S&C INTELLITEAM II 16
8.7 DISTRIBUTED AUTO-SEQUENCER (DAS) 18
8.8 DMS-BASED CUSTOM AUTOMATION 20
8.9 SLECS FAULT DETECTION, ISOLATION AND SYSTEM RESTORATION (FDIR) 22
9. OBSERVATIONS 25
9.1 NETWORK AWARENESS 25
9.2 BACKWARD COMPATIBLE APPROACHES TO DSA 25
9.3 CLOSE-ONTO-FAULT CAPABILITY 26
9.4 DECISION MAKING LOCALE 26
9.5 COMMUNICATIONS 26
9.6 THIRD ORDER SYSTEMS 27
10. PRECEDENCE RELATIONSHIPS 27
11. TIMELINE 28
12. FORWARD COMPATIBILITY REQUIREMENTS 28
12.1 SWITCHING DEVICES 28
12.2 SCADA COMMUNICATIONS 29
12.3 DMS 29

2. Disclaimer

This internal ENERGEX document has been released to the IEEE Working Group on Distribution Automation free of charge on the basis that the information contained will be used for constructive collaboration between ENERGEX and other organisations. The mention of, or omission to mention, specific commercial products does not signify endorsement or otherwise by ENERGEX.

ENERGEX (and its related companies) do not in any way represent or guarantee the accuracy or completeness of the information in this document and you should not rely upon it as accurate or complete.

To the extent permitted by law, ENERGEX (and its related companies) will not be responsible for any loss, damage, costs or expense incurred as a result of any errors, omissions, or representations in relation to the information contained in this document.

The material contained in this document is subject to copyright and may not be dealt with except in accordance with the Copyright Act 1968 (Cth) or as otherwise agreed in writing by ENERGEX.

3. Purpose

Included in the scope of the Distribution System SCADA (DSS) initiative [2] is "*Suitability of equipment for use in future simple DSA systems (forward compatibility)*". This document states ENERGEX's assumptions about future DSA systems, as a basis for determining forward compatibility requirements.

4. Terminology

For a glossary of related terms, see Project Note 1 [1].

Unless otherwise qualified, the word "network" means the electricity network.

The word "configuration" means electricity network configuration or secondary system configuration according to context.

5. Referenced Documents

1. ENERGEX, DSS Capability Project – Project Note 1, *Glossary*
2. ENERGEX, DSS Capability Project Note 3, *DSS Concept of Operations*
3. S&C, Descriptive Bulletin 766-30, *S&C IntelliRupter PulseCloser*
4. ENERGEX, DSS Capability Project – Project Note 17, *Issues List*
5. Staszesky D (S&C), Craig D (Enmax), Befus C (S&C), *Advanced Feeder Automation is Here*, IEEE Power and Energy, September/October 2005
6. Leditschke M (SEQEB), *Distributed Auto-Sequencer (DAS) Reference Manual*
7. SLECS, *Fault Detection Isolation and System Restoration* (extract from DMS user documentation)
8. Electric Power Research institute (EPRI) – *IntelliGrid Architecture*
9. DNP User Group, *DNP3 Specification, Supplement to Volume 7, Secure Authentication*
10. ENERGEX, Network Technology Plan 2005-2025 – Project Note 35, *Executive Summary*
11. ENERGEX, Network Technology Plan 2005-2025 – Project Note 14, *Precedence Relationships in Benefits Realisation - Reliability*

6. DSA Defined

DSA is defined in [1] as "... a vague term used by some to mean Distribution System SCADA (as distinct from Substation SCADA) and by others to mean highly automated, self-healing capability." For the purposes of this document, DSA will refer to automated fault detection, isolation and restoration. This definition turns out to be surprisingly broad, as subsequent examples will show.

7. Differentiating Features

7.1 Scope and Objectives

DSA may be used to target high priority loads or the network in general.

7.2 Granularity

DSA systems may operate at the site, feeder, scheme or system level.

7.3 Decision Making Locale

For the purposes of this Project Note, *decision making locale* refers to the place (or places) at which automated isolation and restoration decisions are made.

- ***Coordinated***: Low-level components operate independently in accordance with settings which have been coordinated at design time.
- ***Distributed***: Low-level components operate independently and collaboratively.
- ***Hierarchical***: Subsystems of lower-level components collaborate via (or are coordinated by) a higher-level system.
- ***Centralised***: Low-level components merely act as the "eyes and arms" of a higher-level system.

This classification takes into account the granularity, which explains why PLC-based autochangeover (see examples in Section 8) receives a classification of centralised – all decision making happens at the highest level for that kind of system, i.e. in the PLC.

7.4 Network Awareness

For the purposes of this Project Note, *network awareness* refers to the ability of a DSA system to adapt to actual system conditions, automatically and in real-time. The following three aspects of network awareness are considered:

- ***Topology awareness*** refers to the ability of the DSA system to find isolation and restoration solutions based on the actual (as opposed to typical or as-designed) network configuration. Topology awareness may be restricted to single and/or non-overlapping events, or broadened to include multiple and/or overlapping events.
- ***Constraints awareness*** refers to the ability of a DSA system to avoid constraint violations such as overload and undervoltage, taking into account actual (as opposed to typical or as-designed) load and ratings. Constraints awareness may be restricted to conditions at the time of operation, or broadened to include predicted conditions.

- ***Protection awareness*** refers to the ability of the DSA system to find main and backup protection solutions for the whole network based on the actual (as opposed to typical or as-designed) network configuration and load. Protection awareness may be restricted to conditions at the time of operation, or broadened to include predicted conditions.

See examples in Section 8.

Network awareness in the most general sense requires that potential solutions be evaluated using load flows and protection studies on a real-time network model. Predictive constraints awareness and protection awareness require the incorporation of load forecasting and dynamic ratings into the network model. Further, protection awareness requires a willingness to delegate the determination and application of protection settings to an automated system. These requirements in turn place unprecedented demands on the quality of network data and system components.

7.5 Standards

If restricted in use, DSA solutions are likely to be customised to each application. If broadly used, DSA solutions are likely to be standardised. The standards employed may be specific to an organisation, to a vendor, or to the whole industry.

7.6 Impacts

The scope and objectives, architecture and standards affect the specifications for system components (power apparatus, communications systems, DMS) and human factors (people and processes).

8. Examples

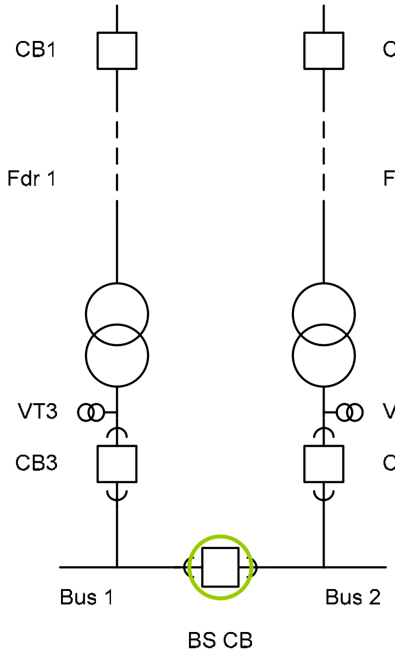
Note: In all of the following examples, feasibility conditions related to equipment ratings, protection, voltage control, communications, etc. are assumed to be met, and "ideal" operation is described.

8.1 Autochangeover and Autorestoration

Deployment:	Widespread
Vendor(s):	Various
Granularity:	Site
Decision making locale:	Centralised
Network aware:	No
Communications:	None
Description:	Refer to Figure 1 (next page)

This application exists in many variations at HV, MV and LV. It can be implemented easily in hardwired components, PLCs and end-user-programmable RTUs. The types of switching devices and sensors can be varied according to specific requirements. For example, if VTs are unavailable then (subject to suitability) local LV supplies may be used for main and/or alternate supply status indication. Additional sensors and checks can be incorporated, eg. to prevent closure onto faults. At MV, an entire scheme can be bundled into a single RMU with motor-operated switches. In Figure 1, it is assumed that the source CB autoreclose settings and the autochangeover / autorestoration settings are coordinated at design time.

Advantages:	Simple, flexible
Disadvantages:	Confined to a single site



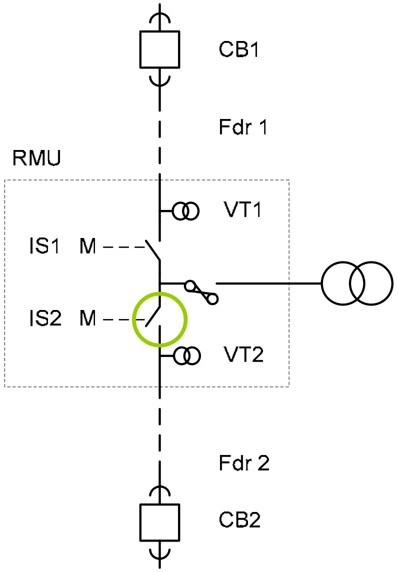
Permanent fault on Fdr 1
(BS CB normally open):

- CB1 trips
- CB3 trips - intertrip
- Bus 1 off supply - VT3
- Alternate supply available – VT4
- CB3 confirmed open or opened
- BS CB closed
- CB1 recloses and locks out

Temporary fault on Fdr 1
(BS CB normally open):

- CB1 trips
- CB3 trips - intertrip
- Bus 1 off supply - VT3
- Alternate supply available – VT4
- CB3 confirmed open or opened
- BS CB closed
- CB1 recloses and reclaims
- Normal supply available – VT3
- CB3 closed
- BS CB opened

(a) Zone Substation Application



Permanent fault on Fdr 1:

- CB1 trips
- Fdr 1 off supply - VT1
- Alternate supply available – VT2
- IS1 opened
- IS2 closed
- CB1 recloses and locks out

Temporary fault on Fdr 1:

- CB1 trips
- Fdr 1 off supply - VT1
- Alternate supply available – VT2
- IS1 opened
- IS2 closed
- CB1 recloses and reclaims
- Normal supply available – VT1
- IS1 closed
- IS2 opened

(b) Distribution Substation Application

Figure 1

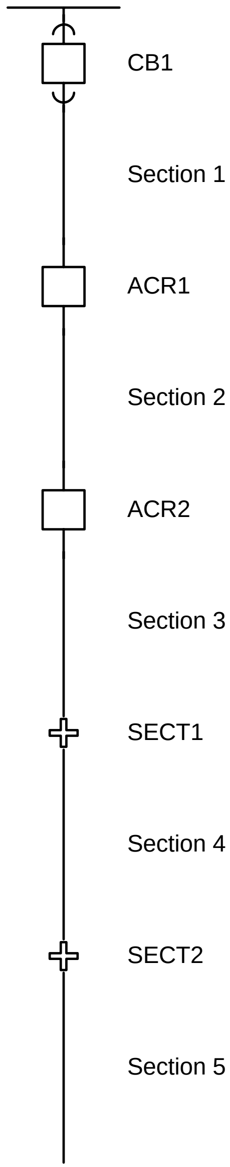
8.2 Automatic Reclosing and Sectionalising

Deployment:	Widespread
Vendor(s):	Various
Granularity:	Feeder
Decision making locale:	Coordinated
Network aware:	No
Communications:	None
Description:	Refer to Figure 2 (next page)

Automatic reclosing and sectionalising are time-honoured measures for improving network reliability. Sectionalisers have no fault interrupting capability. They operate by counting either loss-of-voltage events (*voltage sensing*) or through-fault events (*current sensing*) and opening in the autoreclose dead time. Both sensing methods have unique strengths and weaknesses.

Modern ACRs have bi-directional protection and voltage sensing for coordination in normally closed rings (see also Loop Automation).

Advantages:	Simple
Disadvantages:	The number of reclose shots must be set to one more than the number of downstream sectionalisers; Multiple reclose shots increase the likelihood of secondary damage



Permanent fault in Section 1:
- CB1 trips
- CB1 recloses
- CB1 trips and locks out

Permanent fault in Section 2:
- ACR1 trips
- ACR1 recloses
- ARC1 trips and locks out

Permanent fault in Section 3:
- ACR2 trips
- ACR2 recloses
- ACR2 trips
- ACR2 recloses
- ACR2 trips
- ACR2 recloses
- ACR2 locks out

Permanent fault in Section 4:
- ACR2 trips
- ACR2 recloses
- ACR2 trips
- ACR2 recloses
- ACR2 trips
- Sect1 opens
- ACR2 recloses and reclaims

Permanent fault in Section 5:
- ACR2 trips
- ACR2 recloses
- ACR2 trips
- Sect2 opens
- ACR2 recloses and reclaims

Figure 2

8.3 *S&C IntelliRupter, SpeedNet and IntelliTEAM III*

Deployment:	Unknown	
Vendor(s):	S&C	
Granularity:	Feeder	
Decision making locale:	Distributed	
Network aware:	Topology	No
	Constraints	No
	Protection	Limited
Communications:	Peer-to-peer	

Description:

The most advanced ACR at the time of writing is IntelliRupter from S&C. IntelliRupter is capable of single phase "PulseClosing" – the faulted phase is reenergised for a fraction of a cycle only – enough time for fault sensing but not enough for high energy let-through. When delivered with (embedded) SpeedNet radios and IntelliTEAM III software, a group of IntelliRupters can collaborate to minimise the number of customers affected by a permanent fault – with no practical limit on the number of devices in series down a feeder.

Advantages:	Greatly reduced likelihood of secondary damage; No practical limit on the number of devices in series down a feeder; First product to exhibit protection awareness
Disadvantages:	Proprietary solution; New product with limited field service

(This page intentionally blank)

8.4 Loop Automation

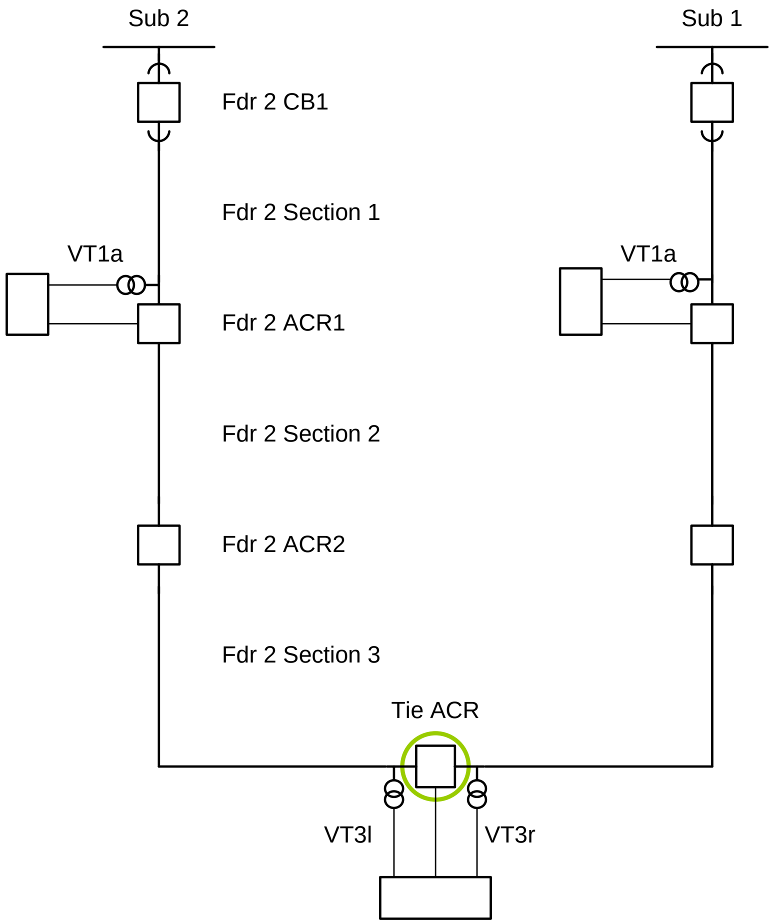
Deployment:	Widespread
Vendor(s):	Various
Granularity:	Feeder pair
Decision making locale:	Coordinated
Network aware:	No
Communications:	None
Description:	See Figure 3 (next page)

Loop automation is an extension of conventional automatic reclosing in which restoration of the tail of the faulted feeder is attempted by closing a tie to an adjacent feeder. The ACRs must be equipped with voltage sensing and/or bidirectional protection, depending on their positions along the feeder.

Advantages:	Simple
Disadvantages:	Multiple reclose shots increase the likelihood of secondary damage

Loss of supply from Sub 2;
Permanent fault in Section 1;
Permanent fault in Section 2;
Permanent fault in Section 3:

Mirror image of Sub 1 / Fdr 1



Loss of supply from Sub 1:
- Section 1 off supply – VT1a
- ACR1 opened
- Section 3 off supply – VT3r
- Alternate supply available – VT3l
- Tie ACR closed

Permanent fault in Section 1:
- CB1 locks out
- Section 1 off supply - VT1a
- ACR1 opened
- Section 3 off supply - VT3r
- Alternate supply available VT3l
- Tie ACR closed

Permanent fault in Section 2:
- ACR1 locks out
- Section 3 off supply - VT3r
- Alternate supply available - VT3l
- Tie ACR closed onto fault
- ACR2 locks out

Permanent fault in Section 3:
- ACR2 locks out
- Section 3 off supply – VT3r
- Alternate supply available – VT3l
- Tie ACR closed onto fault
- Tie ACR locks out

Figure 3

8.5 SP Manweb Urban Automation (UA) System

Deployment:	Scottish Power Manweb
Vendor(s):	Radius
Granularity:	Feeder
Decision making locale:	Centralised
Network aware:	No
Communications:	Master-slave
Description:	See Figure 4 (next page)

Compared with Loop Automation, the UA system avoids the need for a tie ACR through feeder-level coordination to ensure that the tie switch will never be closed onto a fault. Voltage sensing is required at all switch sites. Bidirectional protection is not required. A detailed description of the UA system can be found in [4].

Advantages:	Simple and modular
Disadvantages:	Multiple reclose shots increase the likelihood of secondary damage; Requires communications with the supply point for correct operation

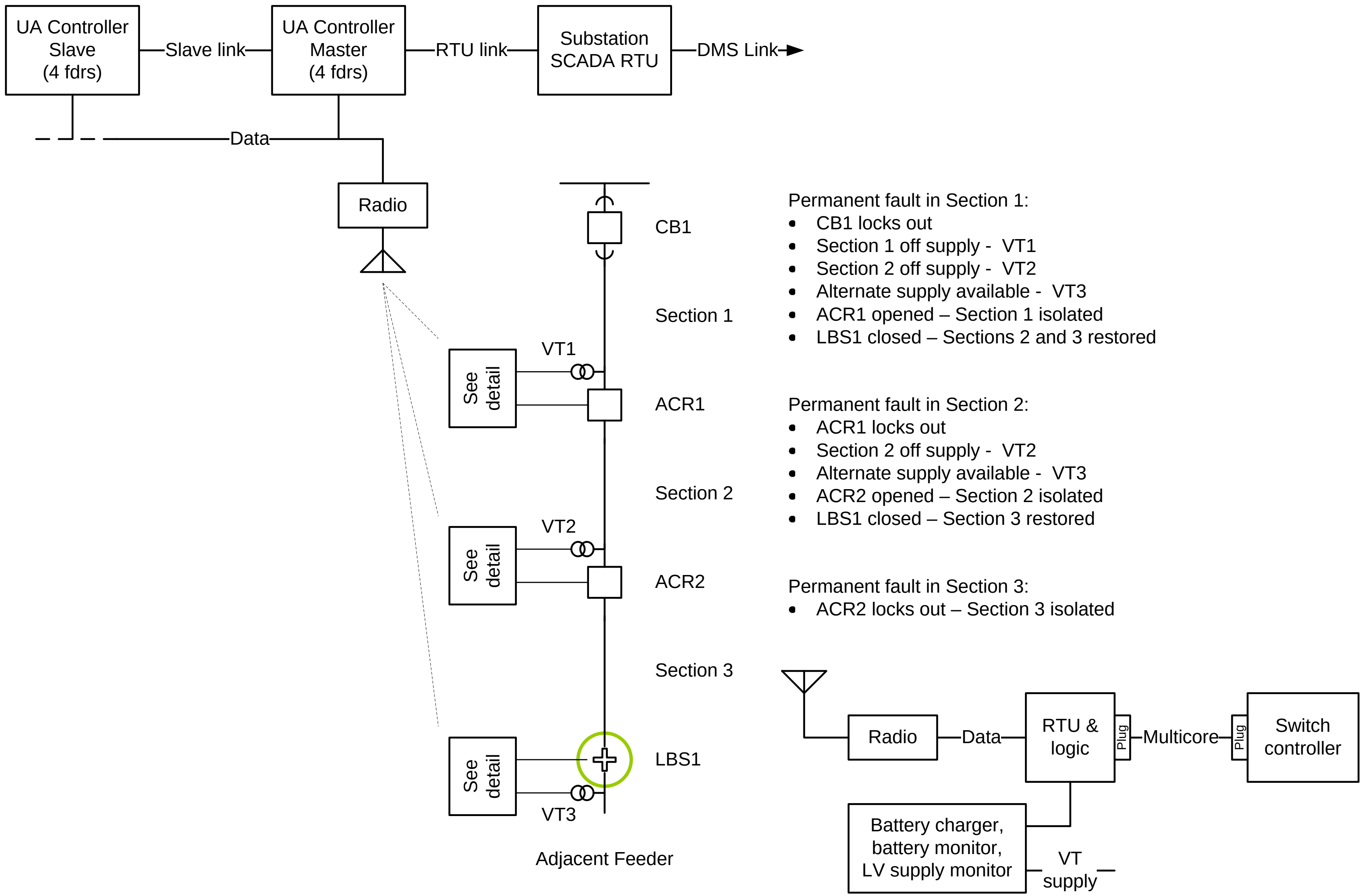

UA Controller Slave (4 fdrs)
Slave link
UA Controller Master (4 fdrs)
RTU link
Substation SCADA RTU
DMS Link
Data
Radio
CB1
Section 1
VT1
See detail
ACR1
Section 2
VT2
See detail
ACR2
Section 3
LBS1
See detail
VT3
Adjacent Feeder
Permanent fault in Section 1:
• CB1 locks out
• Section 1 off supply - VT1
• Section 2 off supply - VT2
• Alternate supply available - VT3
• ACR1 opened – Section 1 isolated
• LBS1 closed – Sections 2 and 3 restored
Permanent fault in Section 2:
• ACR1 locks out
• Section 2 off supply - VT2
• Alternate supply available - VT3
• ACR2 opened – Section 2 isolated
• LBS1 closed – Section 3 restored
Permanent fault in Section 3:
• ACR2 locks out – Section 3 isolated
Radio
Data
RTU & logic
Plug
Multicore
Plug
Switch controller
Battery charger, battery monitor, LV supply monitor
VT supply

Figure 4

8.6 S&C IntelliTEAM II

Deployments:	Various (refer to S&C web site)	
Vendor(s):	S&C	
Granularity:	Scheme	
Decision making locale:	Distributed	
Network aware:	Topology	No
	Constraints	Load only
	Protection	No
Communications:	Peer-to-peer	
Description:	Refer to Figure 5 (next page)	

Quoting the manufacturer's literature [5]: *IntelliTEAM II is a patented automatic power restoration system that uses distributed intelligence and peer-to-peer communication to switch and isolate the faulted line section and restore power to unfaulted line sections. IntelliTEAM II utilizes ties [between multiple feeders], enabling a wide variety of [feeder] configurations to maximize the restoration potential.*

"Team" and "coach" metaphors help to describe IntelliTEAM II operation. Each team is defined as a line segment bounded by two to eight automated switches, each of which can represent a different power source. Each team has a software coach. If an outage or line fault occurs, local control logic determines if a switch should open. The coach of each affected team then uses real-time data, including voltage and current data gathered prior to the system event to develop a restoration strategy for unfaulted sections. The coaches of adjacent teams then work together through shared controls to implement strategies that will maximize restoration of the circuit within the prioritization rules defined by the user.

IntelliTEAM II distributed control algorithms can address multiple contingencies. If a team is in the reconfigured state and the alternate source experiences a new event, the team can look for a new alternate source, if available, to supply its line segment. As long as an alternate is available, some amount of service can be restored. A large IntelliTEAM II system may have reconfigurations occurring simultaneously at more than one location.

Following a reconfiguration event, and subsequent repair and restoration of the faulted line section, team members can return to their normal state.

Advantages:	Advanced concept which addresses the goal of the "self-healing" network
Disadvantages:	Proprietary solution; Requires a peer-to-peer wide area communication network; Configuration data must be distributed to RTUs in conjunction with network changes

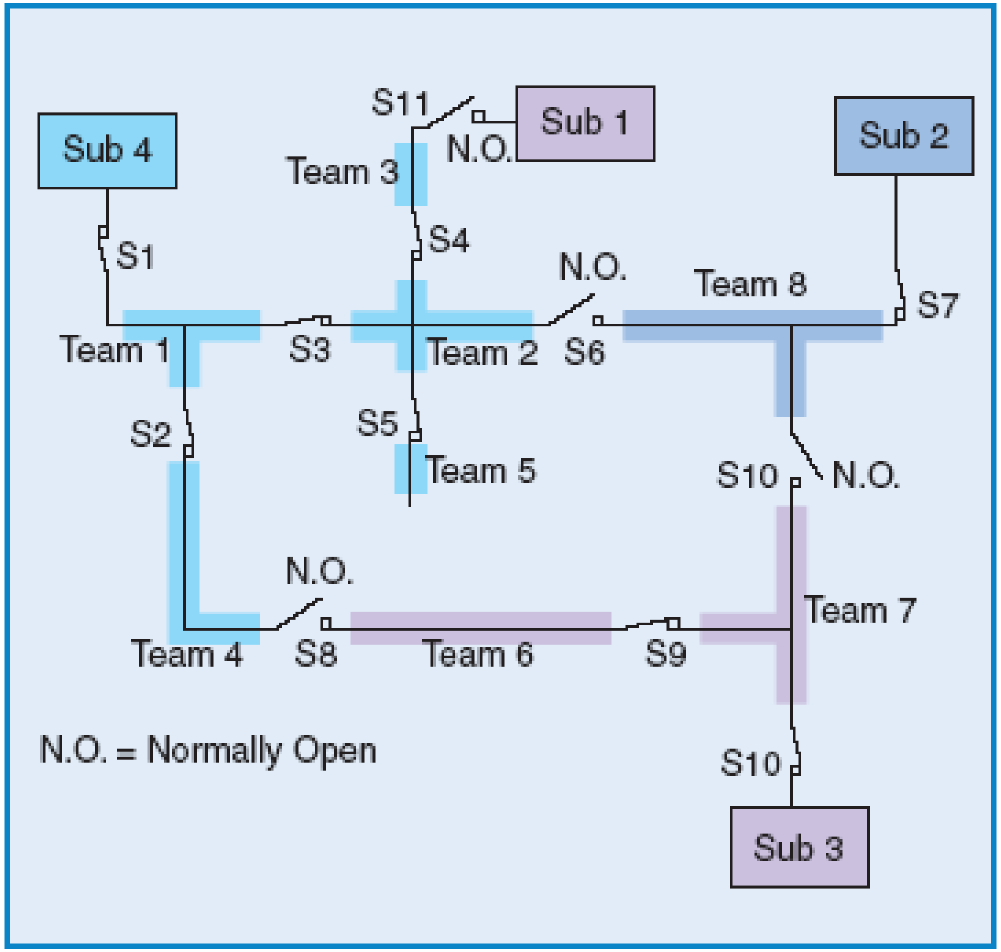


Figure 5 (source [5]) Example of Team configuration for four radial feeders

8.7 Distributed Auto-Sequencer (DAS)

Deployment:	Nil (obsolete)	
Vendor(s):	n/a	
Granularity:	Scheme	
Decision making locale:	Hierarchical	
Network aware:	Topology	No
	Constraints	Load only
	Protection	No
Communications:	Master-slave	
Description:	Refer to Figure 6 (next page)	

DAS was conceived and developed by SEQEB personnel in the early 1990s. It was used to implement a number of multi-site, custom automation schemes. The DAS "engine" was installed in each SACS unit or RDC participating in a scheme. The engine was an interpreter for a hardware-independent automation language. Peer-to-peer interchange between participants took place via an intermediary located at the lowest level in the SCADA communications hierarchy that was common to all participants. Scheme design guidelines encouraged modular design and the exchange of high-level process variables, thus allowing each site to function with maximum autonomy [6].

DAS schemes were phased out with the commissioning of ENERGEX's SLECS DMS in the early 2000s. In many ways, DAS was ahead of its time – a noble attempt to provide DSA capability on the SCADA platform of the day. The tendency to develop complex, highly customised DSA schemes rather than flexible, multiple-use DSA products was a strategic error which contributed significantly to its ultimate downfall.

Advantages:	DAS automation language shielded developers from the complexities of the underlying platform; Ran on existing SCADA infrastructure
Disadvantages:	Proprietary solution; Constrained by limitations of the underlying platform at the time; Crude development environment

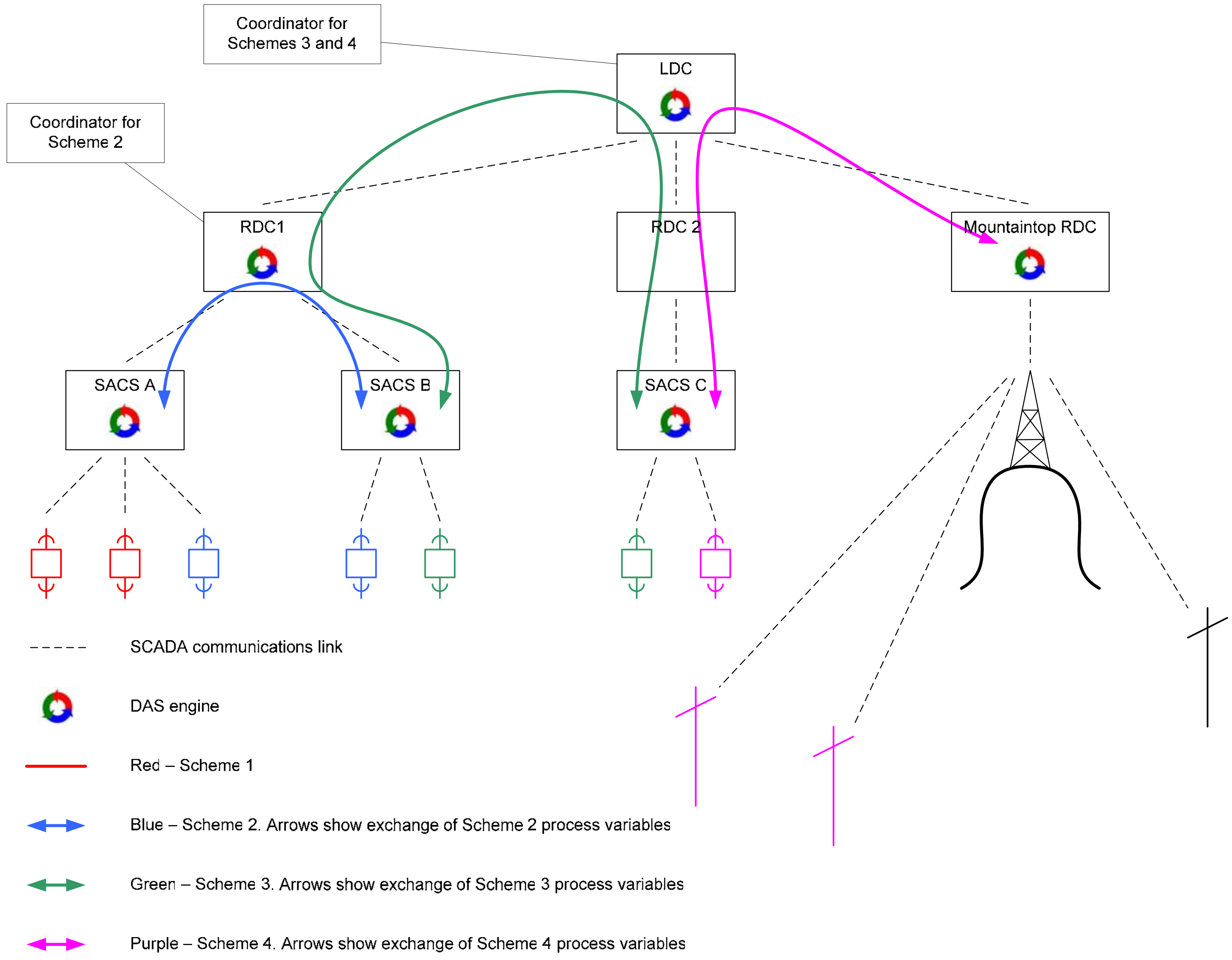

Coordinator for Schemes 3 and 4
LDC
Coordinator for Scheme 2
RDC1
RDC 2
Mountaintop RDC
SACS A
SACS B
SACS C
SCADA communications link
DAS engine
Red – Scheme 1
Blue – Scheme 2. Arrows show exchange of Scheme 2 process variables
Green – Scheme 3. Arrows show exchange of Scheme 3 process variables
Purple – Scheme 4. Arrows show exchange of Scheme 4 process variables

Figure 6

8.8 *DMS-Based Custom Automation*

Deployment:	Widespread
Vendor(s):	Various
Granularity:	Scheme
Decision making locale:	Centralised
Network aware:	Varies
Communications:	Master-slave

Description:

Most modern DMS offerings include a “scripting language” which provides programmatic access to DMS facilities without the need for in-depth knowledge of the platform. An example is the SCADA Command Language (SCL) on the SLECS DMS. Such languages are typically limited in a number of ways, eg. speed of execution; modularity (code, namespace, start/stop); parallelism; volume of executing code which can be supported by the platform. Nevertheless, it is possible to implement custom automation schemes using such facilities.

Advantages:	Programmatic access to network model including configuration, ratings and real-time data; 24x7 platform
Disadvantages:	Limited by the characteristics and performance of the script interpreter; Vulnerable to SCADA communications failures

(This page intentionally blank)

8.9 SLECS Fault Detection, Isolation and System Restoration (FDIR)

Deployments:	Various	
Vendor(s):	SLECS	
Granularity:	System	
Decision making locale:	Centralised	
Network aware:	Topology	Yes
	Constraints	Yes
	Protection	No
Communications:	Master-slave	

Description:

Quoting the manufacturer's literature [7]: *The objective of the Fault Detection Isolation and System Restoration (FDIR) application is to improve customer service by minimizing the duration and extent of forced outages due to faults in the medium voltage (MV) radial network. Whenever a substation breaker or line recloser trips and the associated auto-reclosing relay locks out, the following operations will occur:*

- *FDIR will automatically attempt to determine the location of the fault based on telemetered FRTU fault passage detection and breaker over-current relay trip data.*
- *FDIR will then attempt to identify switching actions that will isolate the faulted section and restore power to [unfaulted] feeder sections upstream and downstream of the faulted section.*
- *FDIR will display the recommended switching actions to the dispatcher for approval and then generate a SCADA Command Language (SCL) script or switching order to perform the switching actions. The dispatcher can also configure FDIR to automatically perform the switching operations without dispatcher approval.*
  ...
- *FDIR can ... automatically generate the switching order that will return the feeder to its pre-fault configuration after the fault is repaired.*

The following are some of the factors and priorities that are considered when FDIR determines the "best" load restoration strategy:

- *Do not cause any new overloads or voltage limit violations beyond a user-specified tolerance. Each strategy is tested with an execution of the Load Flow application.*
- *Restore the entire de-energized island if possible. If this is not possible, attempt to restore as much load as possible by splitting the island.*
- *FDIR normally only considers the network loading condition at the time of execution. There is an optional FDIR implementation that can consider the network loading over the next 24 hours.*

Advantages:	Advanced concept which addresses the goal of the "self-healing" network; Programmatic access to network model including configuration, ratings and real-time data; 24x7 platform; Dynamic adaptation to network changes
Disadvantages:	Proprietary solution; Vulnerable to SCADA communications failures

(This page intentionally blank)

9. Observations

9.1 Network Awareness

- Network awareness in the most general sense requires information that has traditionally not been held in the SCADA environment. In radial systems, loads after reconfiguration can be predicted approximately using simple arithmetic. Voltages after reconfiguration cannot, nor is there a simple, reliable way to determine and apply new protection settings.
- While it is conceivable that the elements required for full network awareness – connectivity model, line and cable impedances, source impedances, ratings, voltage limits and pre-fault quantities – could be updated in real-time to collaborating, distributed devices, such is not considered practical with current technology.
- Even if it were practical, there are no interoperability standards for collaboration between distributed devices, or for real-time updating of configuration data to collaborating, distributed devices. Vendor lock-in would be unavoidable.
- Therefore in any distributed architecture, network awareness will be limited, and configuration management overheads will be significant.
- Network awareness is considered feasible in a centralised architecture. The manufacturer's claims for FDIR include network awareness (for topology and constraints, but not protection).
- The key vulnerability of centralised architectures is loss of SCADA communications. Loss of communications between the "brain" and the "eyes and arms" is disabling.
- Plug-and-play interoperability refers to the ability of a system to automatically detect changes in its fabric, and reconfigure appropriately. Network awareness is an essential step along the path to plug-and-play interoperability, especially for distributed architectures. EPRI [8] calls for plug-and-play interoperability at the primary system device level – an ambitious goal which will only be achieved through global industry collaboration on standards for equipment, software platforms and software services.

9.2 Backward Compatible Approaches to DSA

The DSS Concepts of Operations document [2] lists some gross topological characteristics of the ENERGEX network, and reaches the following conclusions:

- *Ties will be useful for restoration (subject to capacity constraints) in urban areas where, on average, they are located more than half way along the feeders. Ties will not be useful for restoration in rural areas where they are clustered near the supply point.*
- *The use of ACRs in urban areas will be problematic due to protection grading problems (this has been confirmed in practice). Blocking schemes can be used to overcome protection grading problems, however these require fast protection signalling, which does not come cheaply unless pilot cables, optical fibres or high-speed wireless communications are readily available.*
- *The use of ACRs and sectionalisers will be more successful in rural areas where grading is easier.*
- *Accordingly, the DSS reliability improvement strategy for urban areas should be based on manual sectionalising and load transfer, while the strategy for rural areas should be based on automatic reclosing and sectionalising.*

The steps from DSS to DSA will have to accommodate the legacy of these strategies.

9.3 Close-Onto-Fault Capability

A review of the examples in Section 8 leads to the conclusion that closing onto faults, after the initial autoreclose sequence has run to completion, can be avoided. To avert the possibility, fault path information (in the form of through fault indications and/or feeder voltage measurements) must be gathered from multiple sites . In other words, communication of some form is necessary. Given that –

- Closing onto faults should be avoided in order to minimise both safety risks and secondary damage
- SCADA communications is an essential requirement of DSS (the forerunner of DSA)
- The DSS reliability improvement strategy for urban areas will be based on manual sectionalising and load transfer, using the same classes of information that will be required for DSA

– substantial close-onto-fault capability is not considered essential for load break switches, even after the transition from DSS to DSA. Limited close-onto-fault capability (at most a few operations) should be provided to guarantee safety in accidental close-onto-fault events. To back this up, the switches should monitor their own contacts.

9.4 Decision Making Locale

Building on the foregoing, one can conclude that (for ENERGEX) the simplest transition from DSS to DSA involves the acquisition of a DMS-hosted DSA application like FDIR. The most pressing reasons for this are –

- Complex interoperability standards will not be required. Configuration management problems can be solved once and once only by the DMS vendor.
- Network awareness can leverage the DMS network model and pre-existing DMS applications.
- Robustness can be guaranteed (in part) by the 24 x 7 DMS platform.

This is the suggested policy for the short-to-medium term. To adopt it, the need for highly reliable SCADA communications will have to be addressed (see Section 9.5).

As infrastructure capability grows and network performance requirements become more stringent, the balance may shift from centralised to distributed. Further, nothing in this document should prevent the evaluation and adoption of distributed solutions where economically and technically expeditious.

9.5 Communications

- To minimise the risks of automated decision making, high reliability, low latency communications are required. High reliability can be achieved by increasing the intrinsic reliability and/or through redundancy. Low latency can only be achieved through a combination of measures, the most obvious of which is to increase the effective speed of communications.
- To be “reliable,” communications must firstly be “available” – at the place dictated by electricity network needs. In the past, switching device deployment has been constrained by communications availability. To eliminate this constraint, the time and cost to establish or extend coverage will have to be reduced significantly.
- Redundancy (for high reliability) can be implemented in many ways – duplicated networks, alternate networks, mesh networks, etc. The use of redundancy implies the need for middleware to virtualise the endpoints and maintain continuity of service through equipment/service failures and upgrades.

- In distributed systems, the distinction can be made between intra-system communications (used for communications between collaborating, distributed devices) and SCADA communications (used for remote monitoring and control, possibly via one or more gateways). IntelliRupter is the first switching device known to have embedded intra-system communications capability in the form of SpeedNet. This paves the way for assorted collaborative behaviours including unit protection.
- Generally one would expect embedded capability to be dedicated to intra-system communications and not be available for general traffic.
- It is currently unclear whether/how SpeedNet and IntelliTEAM III scale up from a single feeder or a small set of feeders to a whole system. It is clear, however, that both are proprietary technologies that have been developed in a Standards void.
- DSA communications networks will have to support different classes of communications traffic, from low volume/high priority automation data, through high volume/low priority configuration datasets, to online monitoring and configuration management for both DSA equipment and the communications network itself. Given the proposed scale of deployment (of DSS and then DSA), and absenting plug-and-play interoperability in the near term, remote (manual) configuration management and diagnostic capabilities are considered essential for both DSA equipment and the communications network.
- Security of communications is a rising concern, particularly as affordable mainstream technologies (eg. public networks and unlicensed spread-spectrum bands) are susceptible to unpredictable and largely uncontrollable service quality problems.
- Hacking and terrorism also pose threats, which can and should be addressed via encryption, authentication, access control and non-repudiation mechanisms. DNP3 secure authentication [9] is one such mechanism.
- An ideal to pursue into the future will be IP convergence. IP-based technologies will provide a strong platform for future standard plug-and-play network applications. They will also enable the adoption of mainstream standards for important ancillary functions (see Third Order Systems).
- One other important factor must be cited here: The Network Technology Plan [10] notes the central role of communications in the future electricity network. Although embedded, intra-system communications capability for DSA may stand alone, the specification and selection of other communications infrastructure should consider all potential requirements.

9.6 Third Order Systems

- *Third order systems* are to secondary systems as secondary systems are to the primary system – they monitor, control and supervise.
- Mainstream IT has (most inappropriately) usurped the term “Enterprise Management” to characterise systems which manage and monitor ICT infrastructure.
- Anticipating a future in which embedded controllers (in their thousands) have assumed the form of network-connected computing nodes, it is reasonable to assume that mainstream enterprise management technology will be brought to bear.
- However it would be glib to say this without pointing out the complexities: The configuration of the secondary systems will have to follow the configuration of the primary system *in real time*, meaning that a complex fusion of primary and secondary (protection, metering, SCADA, DMS and communications) system configuration management and monitoring will be required.
- This will be the subject of a separate Roadmap.

10. Precedence Relationships

Project Note 14 of Network Technology Plan [11] develops precedence relationships for the realisation of future network reliability targets. Figure 7 (extracted from the Project Note) shows that DSA is a contributor to the sub-goal of “High performance outage management”.

It also details the elements required for DSA, in terms which align well with the foregoing discussion.

11. Timeline

In the Network Technology Plan [10], DSA is scheduled in the 3-7 year time frame, i.e. between 2008 and 2012. This gives time for the realisation of higher priority initiatives and the establishment of key infrastructure.

12. Forward Compatibility Requirements

For forward compatibility with a range of simple DSA systems, the following abridged requirements emerge. These should be used as a guide for the formulation of detailed requirements for procurement specifications.

12.1 Switching Devices

ACR	
Feature	**Comment**
Bidirectional OC (with high-set), EF (with high-set) and SEF protection with trip indication	Basic automation requirement
Bidirectional multi-shot automatic reclosing	Basic automation requirement
Minimum of two setting groups per direction, remotely selectable	To accommodate load transfers after isolation
Voltage monitoring on both sides (tie ACRs)	Needed for automated isolation and restoration after ACR lockout
Voltage monitoring on source side (line ACRs)* * Note: To eliminate a constraint on device orientation (source versus line side) voltage monitoring on both sides is desirable	Needed for automated isolation and restoration after ACR lockout
Pre-fault quantities	Needed for constraints awareness
Open/close control, mode controls, status indications and alarms	Needed for manual control
Standards-based mechanism for remote configuration management and diagnostics	Needed to minimise field visits (in lieu of plug-and-play interoperability)

Sectionaliser / load break switch	
Feature	**Comment**
Bidirectional through-fault indication for OC, EF and SEF	Aid to automated restoration
Bidirectional multi-shot automatic sectionalising	Basic automation requirement
Minimum of two setting groups per direction, remotely selectable	To accommodate load transfers after isolation
Voltage monitoring on both sides	Needed for automated isolation and restoration after ACR lockout
Pre-fault quantities	Needed for constraints awareness
Open/close control, mode controls, status indications and alarms	Needed for manual control
Standards-based mechanism for remote configuration management and diagnostics	Needed to minimise field visits (in lieu of plug-and-play interoperability)

RMU ring switch	
Feature	**Comment**
Bidirectional through-fault indication for OC, EF and SEF (n-1 switches)	Aid to automated restoration
Minimum of two setting groups per direction, remotely selectable	To accommodate load transfers after isolation
Cable-side voltage monitoring	Needed for automated isolation and restoration after ACR lockout
Pre-fault quantities	Needed for constraints awareness
Open/close control, mode controls, status indications and alarms	Needed for manual control
Standards-based mechanism for remote configuration management and diagnostics	Needed to minimise field visits (in lieu of plug-and-play interoperability)

12.2 SCADA Communications

- Fault tolerant system (aggregate of commercial and private components/services) capable of supporting a centralised decision making locale.
- Ability to provide real-time (DSS, DSA) and non-real-time (configuration management) services simultaneously. This implies the need for application-based segregation and prioritisation of communications.
- Ability (where reasonably possible) to provide DSA and non-DSA services simultaneously. This implies the need for application-based segregation and prioritisation of communications.
- Scaleable in cost-effective increments.

12.3 DMS

- Comprehensive network model (connectivity, line and cable impedances, source impedances, ratings, voltage limits).
- SCADA data linked to network model.
- Short-term load forecast.
- Dynamic rating models.
- Load flow and constraint evaluation against proposed network configuration, forecast load and dynamic ratings.

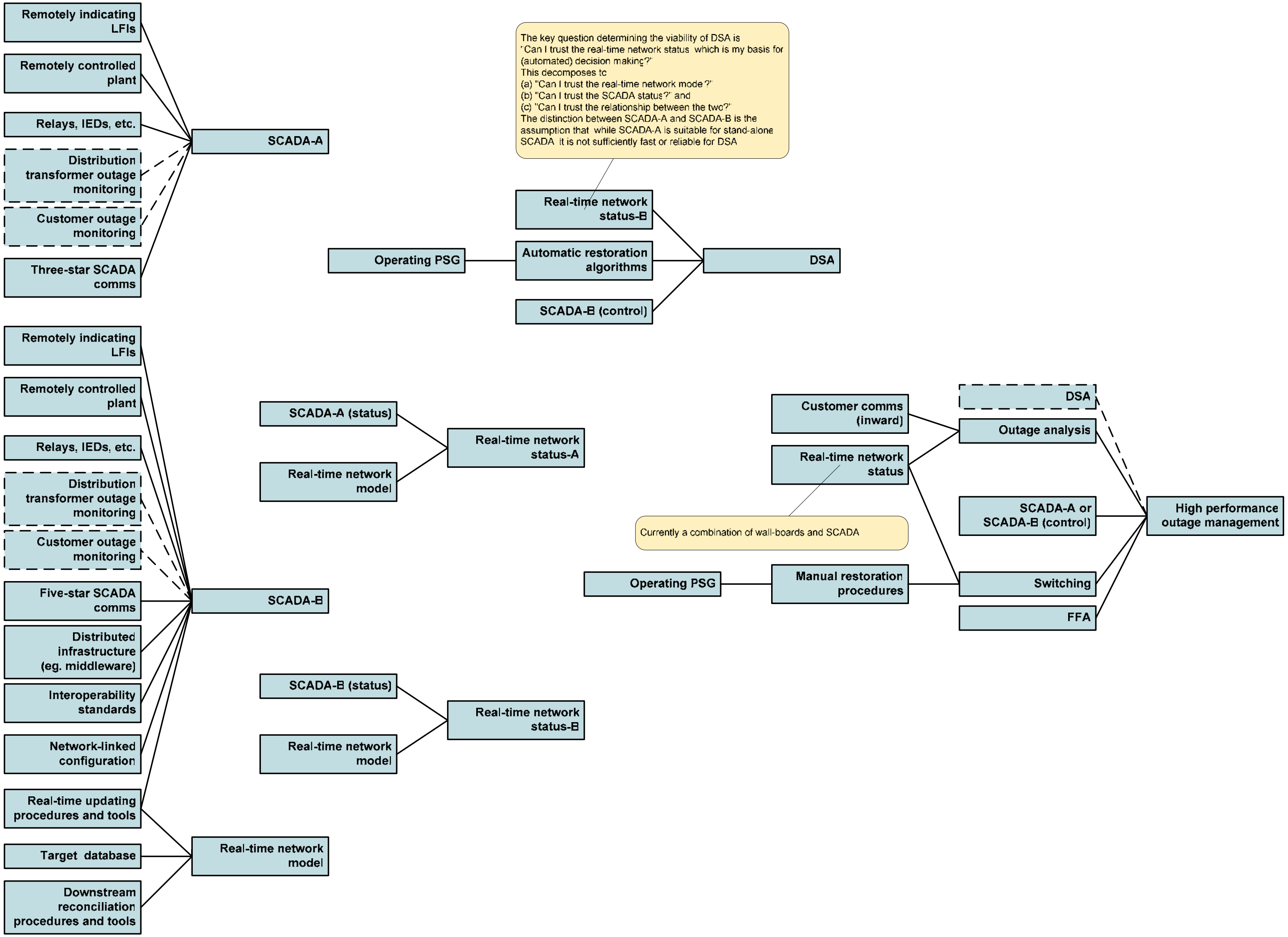

Remotely indicating LFIs
Remotely controlled plant
Relays, IEDs, etc.
Distribution transformer outage monitoring
Customer outage monitoring
Three-star SCADA comms
SCADA-A
The key question determining the viability of DSA is
"Can I trust the real-time network status which is my basis for (automated) decision making?"
This decomposes to
(a) "Can I trust the real-time network mode?"
(b) "Can I trust the SCADA status?" and
(c) "Can I trust the relationship between the two?"
The distinction between SCADA-A and SCADA-B is the assumption that while SCADA-A is suitable for stand-alone SCADA it is not sufficiently fast or reliable for DSA
Real-time network status-B
Operating PSG
Automatic restoration algorithms
SCADA-B (control)
DSA
Remotely indicating LFIs
Remotely controlled plant
Relays, IEDs, etc.
Distribution transformer outage monitoring
Customer outage monitoring
Five-star SCADA comms
Distributed infrastructure (eg. middleware)
Interoperability standards
Network-linked configuration
Real-time updating procedures and tools
Target database
Downstream reconciliation procedures and tools
SCADA-B
Real-time network model
SCADA-A (status)
Real-time network model
Real-time network status-A
SCADA-B (status)
Real-time network model
Real-time network status-B
Customer comms (inward)
Real-time network status
Currently a combination of wall-boards and SCADA
Operating PSG
Manual restoration procedures
DSA
Outage analysis
SCADA-A or SCADA-B (control)
Switching
FFA
High performance outage management

Figure 7