



NAME : Rodney Hughes
COUNTRY : Australia
REGISTRATION NUMBER : 1724

GROUP REF. : SC B3
PREF. SUBJECT : PS1
QUESTION N° : 3

Question 1.3: Is IEC 61850 the right tool for smart grid implementation? Is there already enough service experience to evaluate IEC 61850 for complex systems? What are the consequences for substation operations? Which testing methods are suggested to be applied, in particular for the use in systems like smart grids?

The fundamental principle objective of Smart Grids is to improve **overall reliability and availability** of supply to the consumer at reduced capital and operating cost.

The standardised mechanisms and procedures that are established by the asset owner and required to be included in the Substation Automation System built by the (internal or external) Systems Integrated significantly affect the response times to equipment failures. This significantly affects CAIDI and SAIDI.

Availability is given by

$$A = \frac{MTBF}{MTBF + MTTR}$$

Mean Time Between Failures
Mean Time To Restore

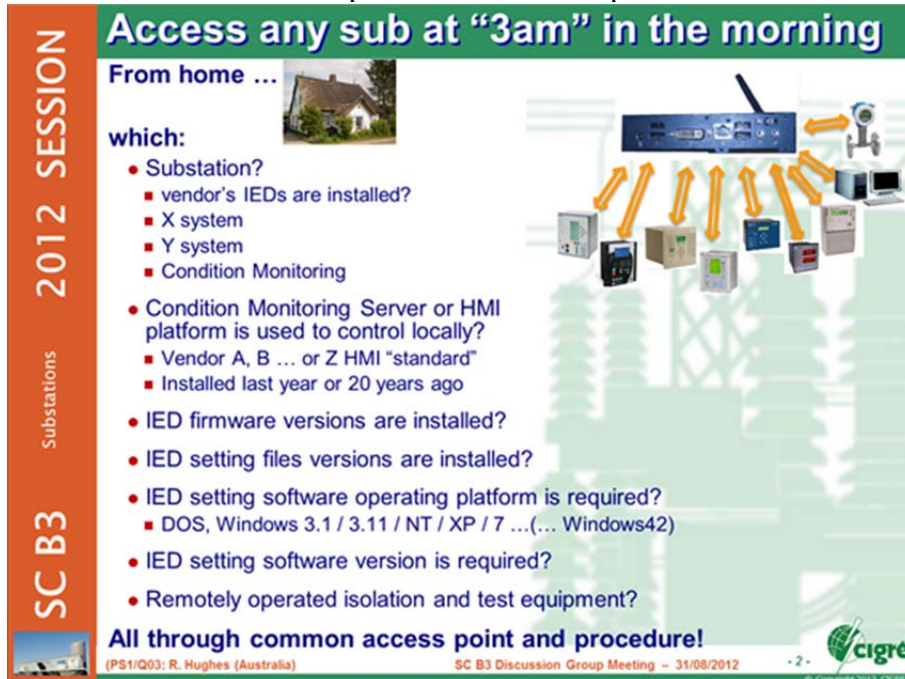
Assuming procurement processes maximise the use of long MTBF equipment, it is also possible to **increase Availability by reducing the MTTR.**

This can be achieved through the use of appropriate systems for technicians and the use IEC 61850 systems

This can be considered in the “**3am in the morning**” scenario for how to respond and fix equipment failures. This is when utility efficiency is most evident.


The first step and priority is for the technician asleep at home or at a friend's party needs to gain remote access to the substation to analyse the situation.

Several difficulties arise in this which prevent effective response:



2012 SESSION
Substations
SC B3


Access any sub at "3am" in the morning

From home ... 

which:

- Substation?
 - vendor's IEDs are installed?
 - X system
 - Y system
 - Condition Monitoring
- Condition Monitoring Server or HMI platform is used to control locally?
 - Vendor A, B ... or Z HMI "standard"
 - Installed last year or 20 years ago
- IED firmware versions are installed?
- IED setting files versions are installed?
- IED setting software operating platform is required?
 - DOS, Windows 3.1 / 3.11 / NT / XP / 7 ... (... Windows42)
- IED setting software version is required?
- Remotely operated isolation and test equipment?

All through common access point and procedure!

(PS1/Q03: R. Hughes (Australia)) SC B3 Discussion Group Meeting - 31/08/2012 - 2 - 

In the worst scenario, the technician doesn't even have any of the required IED operating software on the PC they are using.

The technician therefore needs to be able to use some form of access that guarantees not only security but also that they have full access to the right tools and information specific to the equipment installed at the location in question.

This is best achieved by providing authenticated access to a central server via the corporate LAN/WAN, their PC at home, their Smart Phone or Tablet.

2012 SESSION

Solutions need to provide

Substations

SC B3

Ability to

- Access from any PC mobile device
 - Windows Remote Desktop
- Secure VPN and access control
- Connect to Central Unit
- Select site
- Remotely run software on local substation DCU
 - Virtual Machine for different platform requirements
 - Right software for right IEDs
- Access current site specific files on site server



<http://rodhughesconsulting.com/innovationandsolutions/>

(PS1/Q03: R. Hughes (Australia))
SC B3 Discussion Group Meeting – 31/08/2012
- 3 -

Once logged in to the Central Distributed Control Unit (as for example the DCU provided by 7com Ltd and distributed Rod Hughes Consulting Pty Ltd), this can provide the operator through Windows Remote Desktop (*avoiding need for any special software on their PC) selection and access to the remote site through secure VPN by any variety of communication networks- including Mobile 3G in order to retain segregated or alternative comms to the corporate WAN.

Once connected to the site DCU, the technician can now access the specific IEDs using the IED-specific software installed on the substation DCU. This ensures the right software is available at all times. The DCU can even run Virtual Machine in order to cater for different software operating platform or version requirements.

The substation DCU also acts as a general file server itself providing direct access to documentation and IED configuration files specific to that site.

Using Remote Desktop, the technician operates all these software tools, even accessing other PCs for disturbance records, condition monitoring or even the substation HMI, in order to diagnose the issue and undertake any tasks able to be carried out remotely that may speed up the overall restoration of the equipment.



NAME : Rodney Hughes
COUNTRY : Australia
REGISTRATION NUMBER : 1724

GROUP REF. : SC B3
PREF. SUBJECT : PS1
QUESTION N° : 3

The second issue that faces technicians is the inherent complexity of IEC 61850 systems and messaging.

It is vitally important that the technician has access to the correct isolation procedures and mechanisms specific for that site but which are common standard practice regardless of what equipment is installed.

In the past functions were easily disabled or isolated using the hundreds of links and test points provided in each panel. Isolation simply meant disconnecting the wire-based signals in and out of the particular device under test as may be required for that test.

The “virtual world” of IEC 61850 based systems however carries all those signals over the comms port connection to the IED. Hundreds or thousands of messages will be exchanged between and individual device and all the other IEDs in the system. The IED in question may in fact rely on certain signals from the rest of the SAS and indeed. Some of those other IEDs may rely on certain signals from the IED in question and alarm or revert to a degraded state of operation if those signals are not exchanged even in a test configuration.

We therefore cannot simply disconnect the comms port.











In fact we must implement measures to prevent inadvertent disconnection of the comms ports on the IED and on the network switches.

The process then of “isolating” a function in IEC 61850 is rather a mechanism to **control the operating mode and behaviour of the function or IED** completely **AND that of the all the other functions and IEDs** on the system.

With the same engineering principles and careful consideration for the isolating sequence of the links on the panels, the virtual isolation must deal with all the signals flowing between the Device Under Test and the rest of the system.

Clearly it is unreasonable to expect a technician to do this correctly “on the fly” at 3am in the morning in a substation which he has not visited for several years or not operated the particular IEDs or HMI.

The key elements of any isolation and test facility are

-  Front access (stay away from wires and critical LAN connections in the back)
-  No special equipment (screwdriver)
-  Clear individual labelling
-  Single function control
-  Ease of control
-  Direct feedback indicators
-  Controls clearly related to specific panel
-  Not IED vendor specific
-  Must be as reliable as the system itself (not PC based)
-  **Same in every panel in every substation**

The last is perhaps the most key of them all – we cannot afford to risk confusing the operators and technicians with different and unfamiliar mechanisms to carry out their emergency response tasks (is this relay 3 arrows down, two to the left then press enter or the other way round? This relay doesn't have enough pushbuttons or indicators?)

In addition, mechanisms for virtual systems need to provide extra features such as


- User Role Based Access Control
- Provide human-friendly controls to initiate the sequence of commands and GOOSE messages and verifications to establish the isolation
- System Integrator defined automated sequencing of 'isolation' or function control commands (the SI is the one of few who has total knowledge of all the interactions throughout the entire SAS)
- LAN connection authorisation control for technician laptops and test equipment (no open ports on switches)
- The OTI must be benign on the system – can be replaced 'hot' without itself needing isolation

The patented Operator and Test Interface addresses these issues (licensing available)

<http://rodhughesconsulting.com/innovationandsolutions/>

2012 SESSION

At 3 am in the morning need to ...

From home: 

Gain access

- Physical Connection Authorisation
- Role Based Access Control
 - Specify and procedures for IEEE 1686

Isolate a function


- in the right sequence for that Bay
- Independent of the SAS IEDs
- Independent of which vendor's IEDs
 - Block GOOSE
 - Change a Beh mode
 - Change to SIM mode
 -
- Pre-engineered & configured Operator & Test Interface
 - Patent Registered 2009

Control remotely operated test equipment

Disable faulty equipment

Still keep the system working!!!!

<http://rodhughesconsulting.com/innovationandsolutions/>




Substations

SC B3

(PS1/Q03: R. Hughes (Australia))

SC B3 Discussion Group Meeting – 31/08/2012



© Copyright 2012 CIGRE

The third step to reducing the overall MTTR is providing the technician with facilities that enable **remote restoration** of the equipment, despite an IED being faulty.

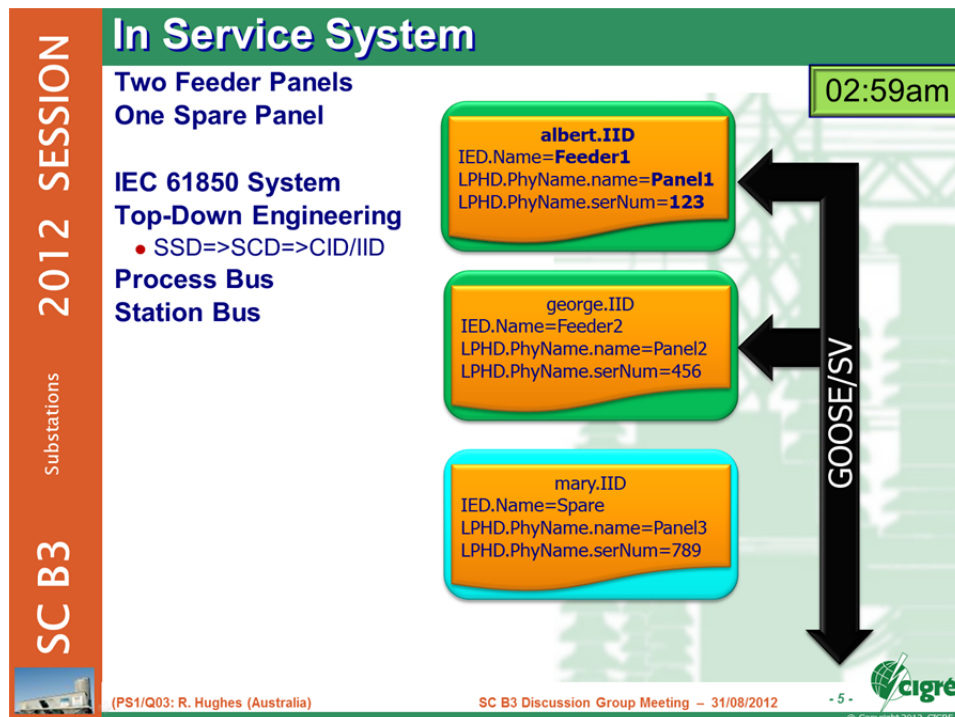
Consider two panels equipment configured for Feeder 1 and Feeder 2. Prior to IEC 61850, i.e. wire based protection systems (regardless of the SCADA technology), it was simply not feasible to re-connect to another Panel all the hundreds of wires connected to each IED specific to that Panel allocation. This would be extremely time consuming and error prone requiring full recommissioning of the system.

If these IEDs are using IEC 61850 Sampled Values and GOOSE (e.g. the Schniewindt conventional CT/VT Stand Alone Merging Unit or other non-conventional instrument transformers and an intelligent CB interface such as the SystemCorp CFE41 IEC 61850 I/O), there are **NO physical I/O to the IEDs** – only the power supply and the communication ports.

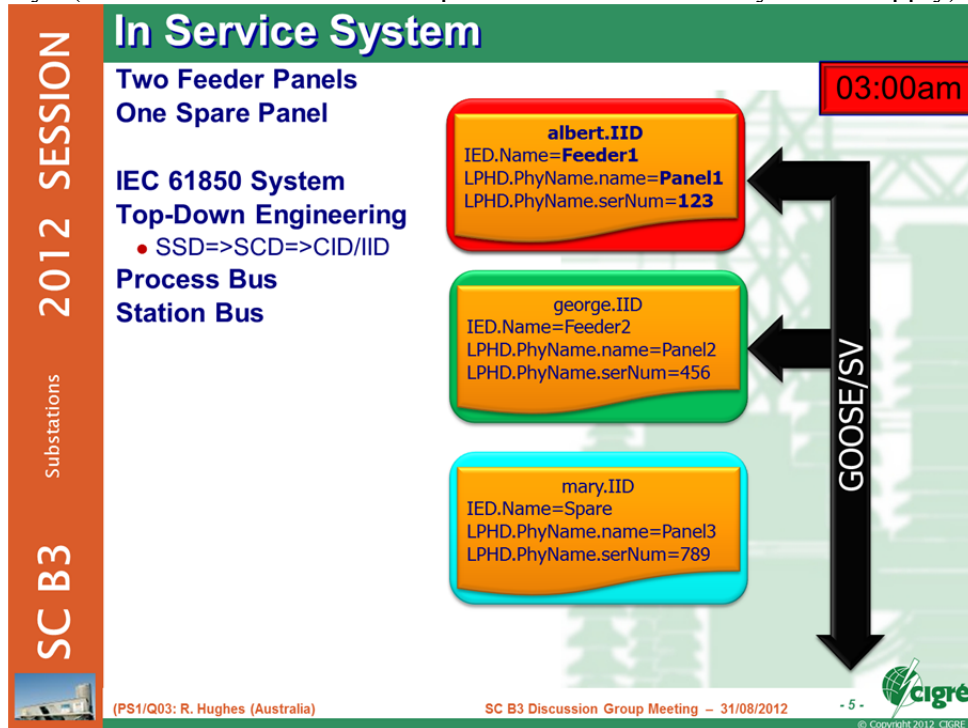
If the utility has also invested in an extra panel providing a complete Spare Panel and IED duplicating any of the actual Feeders, perhaps even a third panel as a spare for the transformer, these IEDs can be reconfigured – locally or remotely - to restore full functionality in “the blink of an eye”.

This requires using the IEC 61850 – 6 Engineering Process and files in a “top-down” process during the initial Specification and subsequent Systems Integration stages:

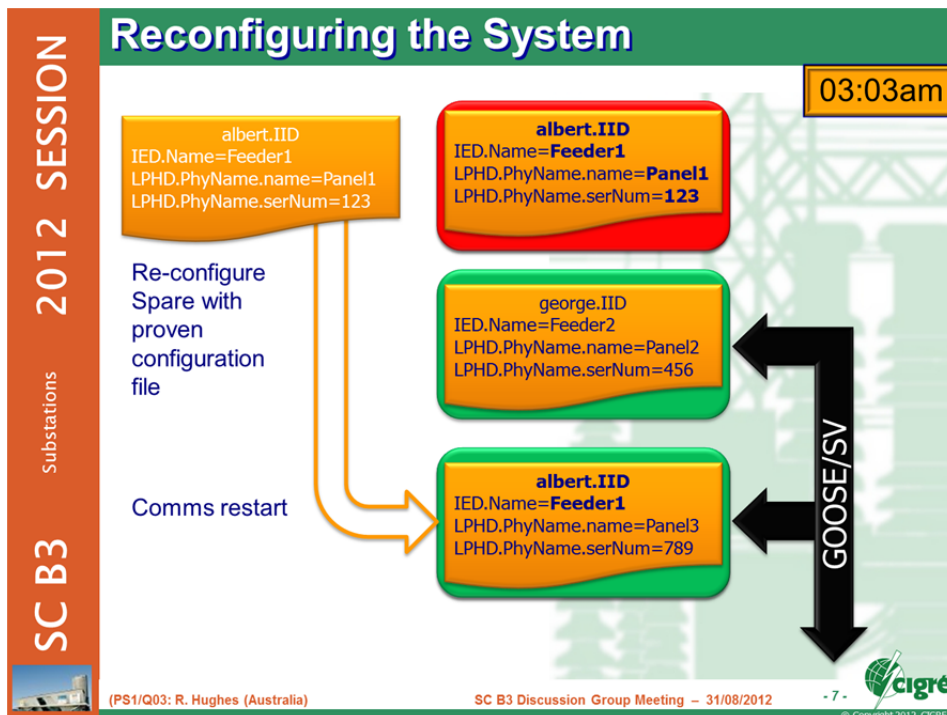
1. **Specifying the system** at the Single Line Diagram level (SSD File)
2. **Systems Integration implementation** (SCD file)
3. **Extract configuration files** for individual IEDs (CID/IID)



If the Feeder1 IED fails for any reason, clearly the substation cannot continue to operate at full capacity. (In the case of a transformer panel several feeders may be off supply).



However it is now possible for the remote technician to obtain the Feeder 1 IID file (*albert.IID*) which is the specific configuration for the protection and control for Feeder 1. This scheme has been fully tested and was clearly in correct operation “just a few moments ago” in the IED on Panel 1 so we have total confidence in its reliability.

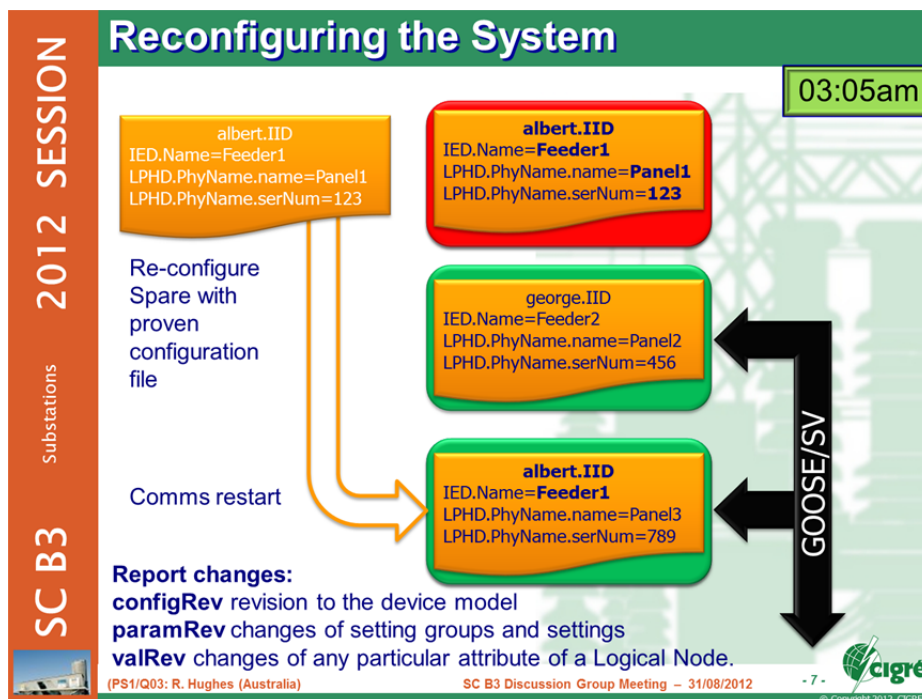


This Feeder 1 *albert.IID* file can now be loaded into the Spare Panel IED previously configured and functionally tested to work (i.e. communicate) with the *mary.IID* file.

Therefore the IED on Panel 3 is now configured with the exact same configuration as was immediately previously operating on Panel 1.

Communications will now be established between all the other IEDs and the IED on Panel 3, returning the entire system to full functionality.

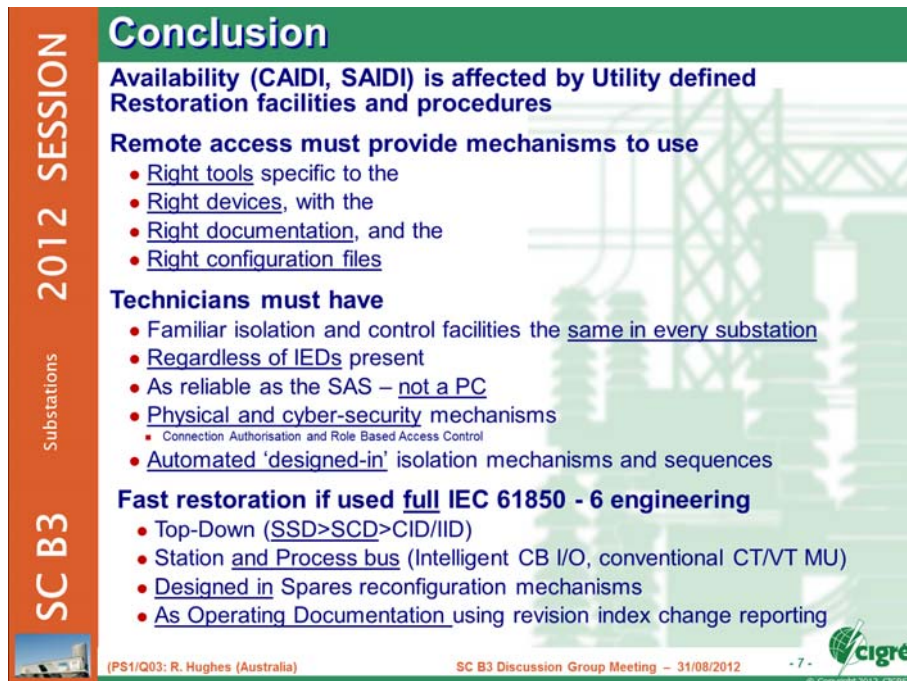
All without the technician leaving home.



The last aspect is to report these changes. This mechanism can be automated if the Systems Integrator originally configures in the design phase some automatic reporting of the three key IEC 61850 revision indices defined in Part 7-3

- configRev
- paramRev
- valRev

Now system control and the protection engineers have complete “**As Operating Documentation**” of the restored system as at “**3:05am in the morning**”



Conclusion

Availability (CAIDI, SAIDI) is affected by Utility defined Restoration facilities and procedures

Remote access must provide mechanisms to use

- Right tools specific to the
- Right devices, with the
- Right documentation, and the
- Right configuration files

Technicians must have

- Familiar isolation and control facilities the same in every substation
- Regardless of IEDs present
- As reliable as the SAS – not a PC
- Physical and cyber-security mechanisms
 - Connection Authorisation and Role Based Access Control
- Automated 'designed-in' isolation mechanisms and sequences

Fast restoration if used full IEC 61850 - 6 engineering

- Top-Down (SSD>SCD>CID/IID)
- Station and Process bus (Intelligent CB I/O, conventional CT/VT MU)
- Designed in Spares reconfiguration mechanisms
- As Operating Documentation using revision index change reporting

Substations 2012 SESSION SC B3

(PS1/Q03: R. Hughes (Australia)) SC B3 Discussion Group Meeting – 31/08/2012 - 7 - © Copyright 2012 CIGRE