NAME : Rodney Hughes
COUNTRY : Australia
REGISTRATION NUMBER : 1887
EMAIL : rgh@rodhughesconsulting.com

GROUP REF. : SC B5
PREF. SUBJECT : PS2
QUESTION N° : Q3

SLIDE ONE (Title slide)

This question goes straight to the point of the need for security in protection and control systems

In fact, CIGRE has published several Technical Brochures under the SC B5 and SC D2 banners on the cyber security aspects of the implementation of IEC 61850, all available through the e-cigre on bookshop shop with member organisations benefitting from free download at all times.

SLIDE TWO

Whilst cyber-security is essential, and part of that is the security/ reliance on time synchronisation is equally a point of concern, we should also consider just what is the risk associated with implementing security on the time synch signals – i.e. what problems do we need to prevent/solve?

Essentially GOOSE does not rely on any time stamp and hence does not rely on having any centralised time, synchronised or otherwise. In fact GOOSE will operate quite happily if all IED clocks are operating independently and are giving time stamps as being years apart!

A message is sent and it is received. Time stamps are irrelevant.
This is just the same as old electromechanical relays did not know what the time was, but they still operated correctly.
The receiving device only cares if the message did not arrive within the TimeAllowedToLive as the duration between one message and when it can expect the next message.

There is a time stamp in the Ethernet header called “T”, but that is the time stamp of when that particular message was created by the IED and pushed onto the LAN. Noting that GOOSE is a repetition sequence, a particular message may be a repeat of an event a year ago, and even then the event may have been a change of an element of no consequence to the subscribing IED.

Whilst it is possible to add the time stamp of the particular event to the dataset, this is really only useful for Sequence Of Events records and aligning one event with another during investigations. Synchronisation of the IED clocks is important in that respect but generally to a 1 millisecond coherency, and may need to be considered as between substations as well as within the substation.

So spoofing the time synch has no effect on GOOSE operation, just event investigations.

SLIDE THREE

Sampled Values has an inherent requirement for synchronisation.

However the Sampled Value messages don't inherently hold the precise time of when a sample was taken.

The requirement is that the Merging Units must all start a timing window of one second duration at porecisely the same instant every second

The SV message then only contains the sample number within that 1-second window e.g. on a 50 Hz system at 80 samples per cycle, each MU must provide a SV at the 5 ms mark (1/4 cycle) of the first cycle with seqNum = 20.
Precisely 20 ms later at the 5 ms mark of the second cycle they must all provide a sample with seqNum = 100

At the end of the 1-second window, the seqNum is reset and the counter starts again.

However time coherency in regards to the start of a 1-second window is CRITICAL, regardless of what the real time is thought to be

So again we see that spoofing the real time has no effect on SV … just as non-IEC 61850 CTs, VTs and relays had no requirement for time synchronisation

So that leaves us with MMS
Here again the only concern is in relation to Sequence of Events being reported out of alignment with other sources.

The overall conclusion is therefore that whilst we must provide security to prevent changes in IED configuration, including configuration f the time clocks, spoofing of the real time being distributed by the clocks has limited impact on the real-time performance of GOOSE, Sampled Values and even MMS. However post fault investigations can be severely hampered, even misled, if there is not correlation of time stamps of events being applied by each IED