ANU CSIP-AUS Conference
OEM Support Day

Fronius Australia, 01.09.2025 – Rod Dewar – Head of Solution Management AU

Experiences with CSIP-AUS

“Learnings from process to date”

“Pain points and issues experienced”

“Suggestions for other beginning their journey”

“Suggestions for improving the CSIP-AUS framework”

Pain points and issues experienced

Standard can be sometimes “too” open

It allows for flexibility, but this can lead to having to implement multiple ways of performing certain functions.
E.g. parallel controls, 2 controls within one DER Control compered to 2 x separate DER Controls in parallel

Randomisation is complex to implement

Were too many documents to read and follow (DSNP Handbooks)
Centralised approach will improve this

Capability Test of each DNSP is different

Suggestions for others beginning their journey

The big question…. Implement **“Aggregator”** or **“Direct on Device”** model

Aggregator

- SW patches easier and faster to deploy
- Additional features easier to deploy
- More difficult for Utilities as they have to deal with a lot more connections. Differences in device models and SW versions etc
- More control of the data flow to the devices
- Legacy devices potentially more likely be able to be included in 2030.5 controls as inverter controls commands using OEM protocols
- Subscription notification can be used
- Inherently potentially more insights and overview of what is happening with the fleet
- Certificate handling likely easier. E.g. Synergy requirement file CSV

Direct on Device

- Data costs, depending on how this is done
- Potentially better for customer if OEM no longer around. (this is questionable though)

Suggestions for others beginning their journey

Build good fleet monitoring tools to recognise problems early

Have adequate local support teams

Run training sessions for installer on how CSIP-AUS works

Suggestions for improving the CSIP-AUS framework

Narrow down the requirements, make more specific

More involvement & influence on the main standard

Perhaps DNSPs could have less aggressive fallback control levels

Have less documents, have DNSPs align more with their requirements

Clarity on who is using 2018 vs. 2023 version of 2030.5

e.g. overlapping schedule handling