Alert loss during DCC Scheduled Maintenance

Update on Feb 2020 actions

Chun Chen (DCC) &

Anik Abdullah (SECAS)

Agenda

- Recap EUK of Problem Statement
- Points of Failure and Solutions
- HAN reliability – Understanding the Impact
- Use of BCDR Environment
- Service User Critical Alerts
- Summary
- Next Steps & Way Forward

EUK Problem Statement Recap

SEC
Smart Energy Code

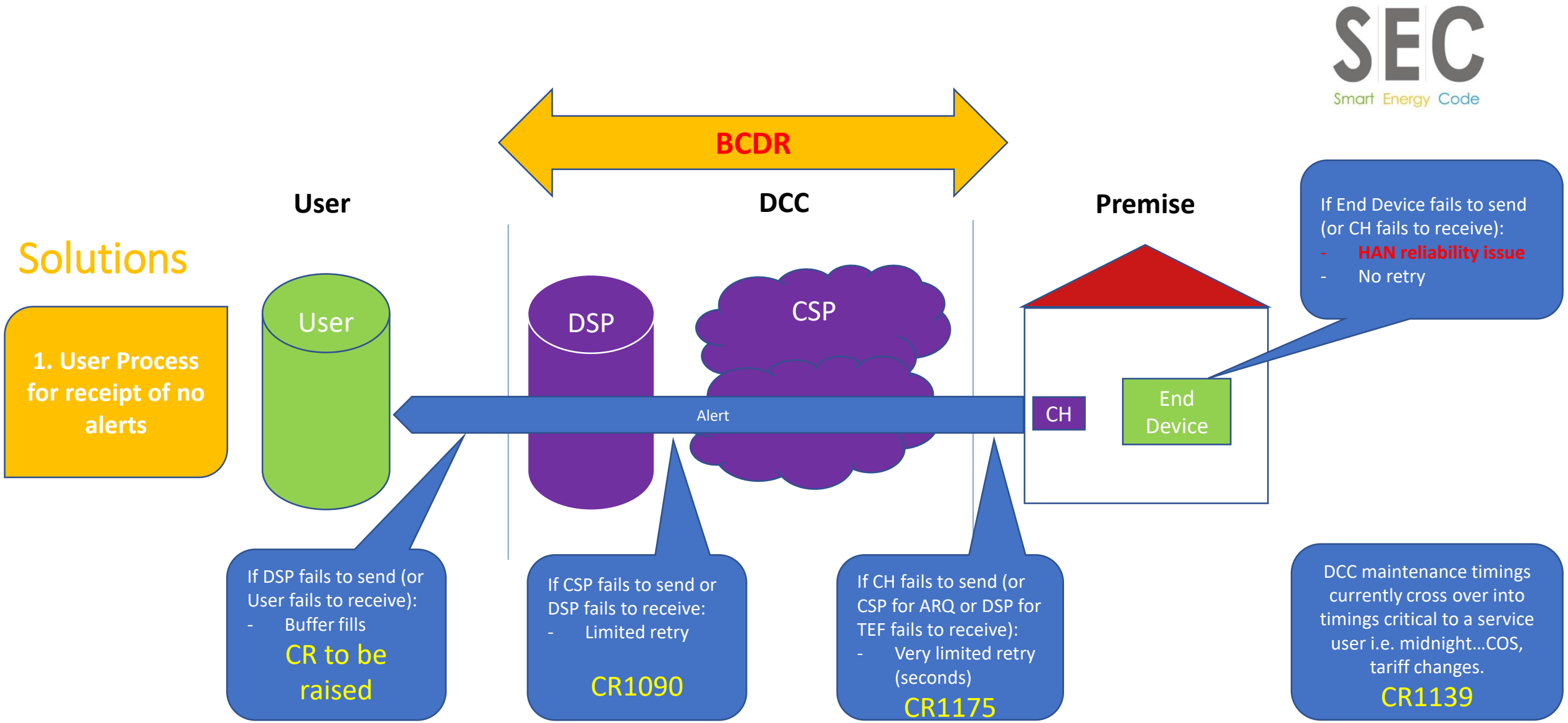
- Cannot guarantee 100% delivery of every Alert. Examples:
  - GSME Alerts during power outages
  - Comms failure beyond designed retry

- Alerts lost during planned maintenance must be avoided
- Alerts lost during unplanned (but scheduled) maintenance must be avoided

} Identical from a DCC design perspective – 'scheduled' henceforth

- Alerts lost in disaster / major incident situations should be minimised (via BDCR)

Points of Failure and Solutions (Generalised)



HAN Reliability - Understanding the Impact

SEC
Smart Energy Code

- If a Device drops from the HAN, this will:
  - At point of Device alert being generated: Device alert is not delivered to CH
  - After the Device re-joins the HAN: Device typically will not retry delivering the alert.

  Resulting in alerts not received by the service user.
- Following a GBCS Alert could allow for monitoring of the HAN reliability issue:
  - 8F84: Failure to Deliver Remote Party Message to ESME (GBCS2.x + CH)
  - 819D (GSME Command Not Retrieved (GBCS1.x)
  - 819E (Tap Off Message Response or Alert Failure (GBCS1.x)
- Following a DCC Alert could also allow for monitoring of the HAN reliability issue:
  - For DUIS2 Customer, N53 alert (Command not delivered to ESME) is generated as a result of 8F84, and sent back to request originator (service user)
  - 819D and 819E which targets ACB and is currently being dropped by DSP/DCC

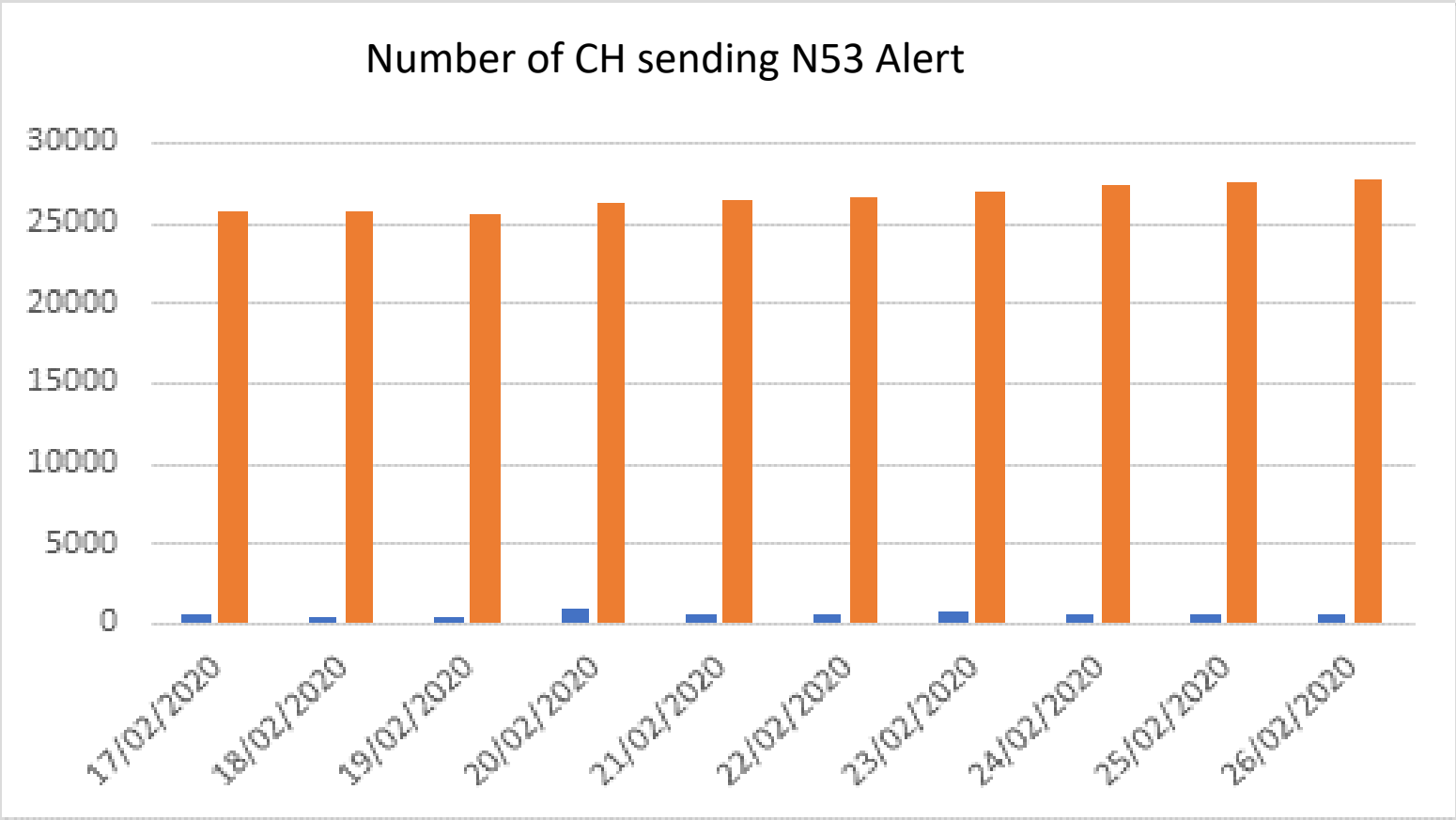
HAN Reliability - Understanding the Impact

SEC
Smart Energy Code

- To monitor the HAN reliability issue, DCC produces an internal daily report on 8F84/N53 recorded from the previous 24 hours.
- This report shows:
  - Device(ESME) dropping off the HAN in the CSP Central & South Region
  - EDMI CH not yet supporting GBCS 2.x, as a result no N53 alerts are being generated by these CH
  - A mix of Comms Hub and Meter problems that are having an impact on the total volume of devices dropping off the HAN
- The root cause analysis is still on going
- A weekly industry communication issued every Friday to the below:
  - **For the attention of Lead Party contacts, Back-up Lead Party contacts, All Service Providers, All Incident Contacts and All Problem Management Contacts.**

Weekly Comms on HAN reliability issue.msg

HAN Reliability Issue - Understanding the Impact



- For this particular weeks data (400-900) CH sent N53 for the first time each day.
- N53 cumulative totals do not increase at expected run rate due to reboot activities.

HAN Reliability - Understanding the Impact

SEC
Smart Energy Code

- Current workaround while the RCA is ongoing
  - DCC TOC daily report provided to the CSP (Central & South) Service Desk.
  - CSP (C&S) executes a remote reboot on the newly identified alerting CH's.
  - Specific details of the affected devices are shared with customers on the DCC SharePoint site (Incidents Folder).
  - Following initial reboot attempts:
    - 75% devices restore service.
      - 70% : CH Silab stack issue (PBI000000118613, APS ACK and link status issue)
      - 30% : other CH/Meter Tunnel stability issues.
    - 25% devices remain failed (The cumulative impacted base is growing by approximately 140 per day)
      - RCA still ongoing, current analysis continues to indicate that meter related issues cover the majority of these drops
- The detail of the Current Root Cause Analysis is provided in the weekly comms

Use of BCDR Environment

- **Current SEC obligation**
  - RTO = 8 hours - See SEC H10.13 (b), but with a target of 4hours, and a minimum service level of 8hours
  - RPO = 15 minutes (i.e. no more than 15minutes of data lost before the disaster). Referenced in SEC H10.13 (c).

- TEF:
  - Active/Active switching is currently limited to the TEF network component
  - However some components will have RTO of 4 hours with Active/Passive as Resiliency mechanisms, this includes Security, and Smart m2m
  - CSP alerts such as AD1 is part of Smart m2m, Device monitoring and management (DMM) component, uses Active/passive across sites as Resiliency mechanisms
  - Both fail over and fail back is achieved by a manual process that:
    - Re-routes the traffic to the standby data centre. This requires the reconfiguration of the load balancers that distribute the traffic to the CSNs.
    - Configures the load balancers to re-route the traffic back to the designated active data centre
  - CR1139 is aimed to resolve the gap for loss of AD1 alerts during TEF scheduled maintenance.

Service User Critical Alerts

- An action was taken at the last TABASC for members to make DCC aware of alerts which were deemed critical by service users
- Steer was given to include those that support the safety of customers and security of operations.

Proposed List:

0x8F78 Unauthorised Physical Access – Other – Supplier
0x8F77 Unauthorised Physical Access - Second Terminal Cover Removed – Supplier
0x8F76 Unauthorised Physical Access - Terminal Cover Removed – Supplier
0x8F74 Unauthorised Physical Access - Meter Cover Removed – Supplier
0x8F73 Unauthorised Physical Access - Battery Cover Removed – Supplier
0x8F3F Unauthorised Physical Access - Tamper Detect – Supplier
0x8F1F Low Battery Capacity – Supplier
0x8F1D GSME Power Supply Loss – Supplier
0x81C0 Supply Disconnect Failure – Supplier
AD1 Power Outage – DNO
0x8F36 Power Restore – DNO
0x8F35 Power Restore – DNO

Some Suggestions:

Prepay Alerts – Fraud and Business Critical.

Indicators of Financial Distress (prepay) - Emergency Credit, Credit Below Threshold, Low Credit

Safety related (Installation) – Reverse Flow, Inc Polarity, Reverse Current.

Summary

SEC
Smart Energy Code

- **Initial study into reliability of HAN throws out a couple of points:**

a) This is a complex area to map, with different root causes and points of failure.

b) However, there is some evidence to suggest the problem is centric to CHs and Devices.

- **Use of BCDR environment**

BCDR is a potential option to tackle loss of alerts during scheduled maintenance if active-active switching is implemented. However, not all components of TEF support active- active switching. ARQ still being investigated.

- **Critical Alerts**

A proposed list of alerts shared with the TABASC, additions have been suggested by members relating to prepay activities, safety (install perspective)

Next Steps & Way Forward

1. Should HAN reliability be investigated as a separate issue?
2. Steer on list of critical alerts/ areas to focus on?
3. Any other solutions to be put forward?
4. Business case for change or fix?
5. A steer on any options presented at TABASC?