RETAIL ENERGY CODE

R0096 – CSS MESSAGE REGENERATION FUNCTIONALITY

WHITE PAPER

BY: FINN DEACON

SIGNED OFF BY: APRIL HARBOUR

1. CHANGE PROPOSAL SUMMARY

Since CSS Go-Live, there have been incidents where the Central Switching System (CSS) has failed to generate messages and therefore are not delivered to the intended recipient. This results in a failure of the Switching process and can cause significant complications for the intended recipient, who is required to manually intervene to re-synchronise messages.

CSS does not currently have the ability to generate messages that were not originally created, such that it is currently unable to perform message synchronisation by re-generating messages.

Change Proposal R0096 has been raised to explore the introduction of new functionality which will allow CSS to identify and re-generate messages which have failed initial generation. For the avoidance of doubt, this Change Proposal does not include any fixes to known incidents that result in messages failing to generate, but looks to introduce functionality that will address incidents as they occur for the enduring CSS operations.

2. BACKGROUND

The Technical Design Authority (TDA), CSS Provider, Gas Retail Data Agent (GRDA) and Electricity Retail Data Agent (ERDA) initially discussed and baselined the requirements for R0096, as part of a Technical Change Workshop. The workshop outputs focused on requirements definition and remained relatively solution agnostic ahead of the Preliminary Impact Assessment (PIA).

However, during the development of this Change Proposal, the CSS incurred a P1 Incident (INC0216074) resulting in secured active and inactive messages relating to consumer switching not being issued out to Market Participants and other parties such as Central Services.

As a result of this incident, the TDA issued a second PIA to capture additional requirements which were identified following the resolution of this incident. However, following the completion of the second PIA, there was still some concern as to whether sufficient time had passed to fully understand and incorporate the findings from the P1 incident. As such, the Change Proposal was put on hold to allow the CSS Service Provider to fully assess the P1 incident and provide an updated approach with regards to a solution.

Following this, it was agreed between the CSS Service Provider and RTS in November 2024 that design up front would be utilised. This was subsequently completed in June 2025, along

with the DIA being returned to RTS in August 2025. Since then, further solution refinement has taken place, leading to the solution's current form.

3. IMPACT OF THE P1 INCIDENT

During the development of this Change Proposal, the CSS incurred a P1 Incident (INC0216074) resulting in Secured Active and Inactive messages relating to Consumer Switching not being issued out to Market Participants and other Parties, such as Central Services. The P1 incident impacted circa 193,000 Registrations which did not successfully progress to Secured Active Registrations, and circa 9,000 Initial Registrations. Similarly, from a Gas perspective, 80,000 Registrations were impacted. As a result, the end Consumers did not have their Switches fulfilled on the planned Supply Start Date. This meant end Consumers were still with their previous Supplier, and blocked from Switching again, until the incident was fixed. Although P1 incidents of this nature are required to be resolved within 4 hours, DCC reported it took 1,606 hours in this instance, significantly impacting industry Parties and end Consumers. Significant costs were incurred across industry to introduce manual interventions, data rectification, reconciliation activities, address customer-raised incidents and mobilise resources from July-August 2023.

4. SOLUTION

The updated approach for a solution has now been provided by the CSS Service Provider which considered the following points around Operational aspects:

- Implementing message regeneration to minimise the downstream impact of message notification failures in the CSS;
- Recognising the importance of identification and where necessary, re-triggering workflow operations that have encountered challenges, such as those stemming from a BCDR (Business Continuity and Disaster Recovery) incident or any other disruptive event that could potentially hinder the delivery of notifications to recipients; and
- Regenerating notifications - CSS must be capable of identifying workflows that have not reached the desired state and instigate automated recovery with manual intervention as a last resort.

This solution has been developed with two key objectives in mind:

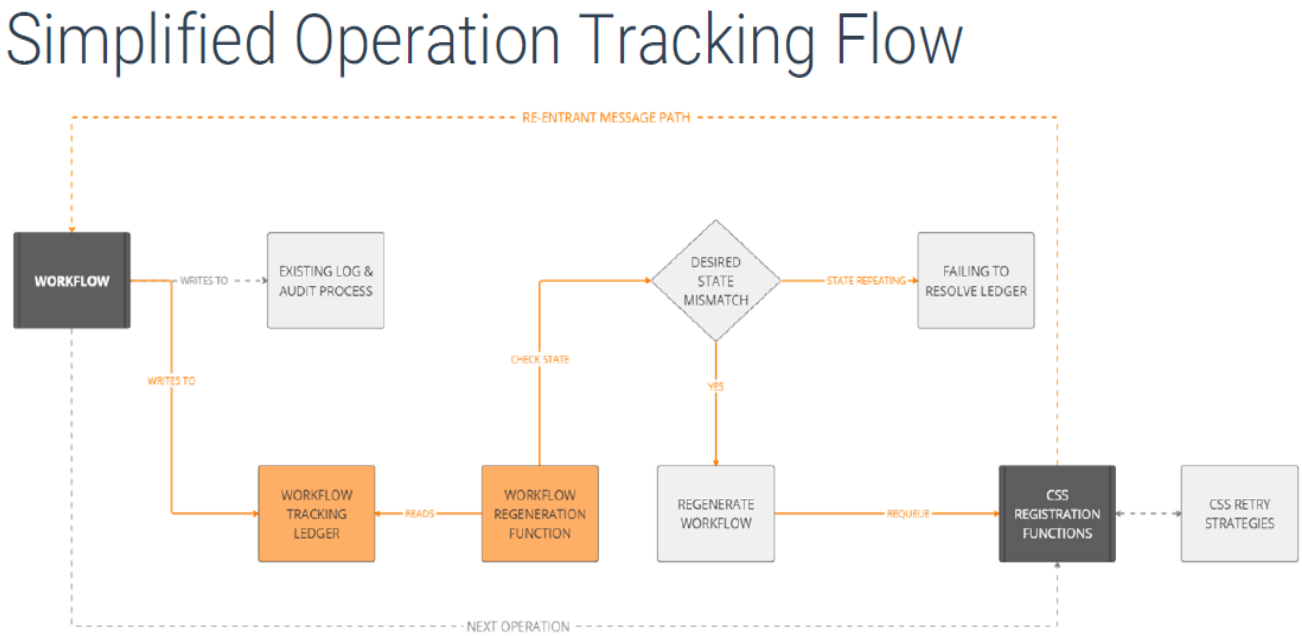
a. To improve the resilience and reliability of the CSS,
b. To mitigate the impacts of similar incidents to that of the P1 incident in summer 2023.

An overview of the workflow for the updated Operational solution approach is provided below and was also shared during a Technical Change Workshop. The solution consists around the following additions:

- Workflow Tracking Ledger – Will provide information of the current workflow state
- Workflow Regeneration Function – Will compare the current workflow state against the desired workflow state

If there is a mismatch between the ‘current’ and ‘desired’ workflow state, this will initiate the ‘Regenerate Workflow’ as a means of the system attempting to ‘self-heal’.

In addition to this, a ‘Failing to Resolve Ledger’ has also been incorporated into the solution and the aim of this is to provide live insight into the Workflow Ledger. This information will be monitored through a live dashboard and therefore provide early notification to the Service & Operations teams of potential and realised failures. The simplified workflow for the solution is illustrated in the image below:



5. ROBUSTNESS OF THE SOLUTION

R0096 implements a new foundation within the CSS architecture to manage Recovery Point System (RPSys), which is designed to significantly enhance operational resilience, recoverability, and observability within the CSS. The robustness and future-proofing of the solution are grounded in strong architectural choices, platform-native design, modern distributed systems patterns, and proactive consideration of scaling, security, and future enhancements.

The key reasons for the robustness of the R0096 solution are detailed below:

- The solution follows 13 defined architecture principles, including cloud-native first, security by design, resilience, idempotency, observability, modularity, and scalability These principles underpin every component of the RPSys and ensure long-term maintainability and adaptability.

- The design leverages Microsoft Azure's enterprise-grade managed services:

Component	Technology	Future-proof benefit
Recovery Point Ledger	**Cosmos DB (multi-region write)**	Automatic global replication, high throughput, 99.999% availability, horizontally scalable
Messaging	**Azure Service Bus Premium w/ Geo-DR**	Deduplication, DLQ handling, high resilience, and built-in failover patterns
Orchestration	**Azure Functions (serverless)**	Auto-scaling, event-driven change-feed triggers, cost-efficient operations
Analytics	**Cosmos Analytical Store + Synapse + Power BI**	Real-time analytics without impact on live systems; scalable for new insights and regulatory reporting

This means the solution inherits platform evolution, security improvements, performance enhancements, and built-in disaster recovery capabilities over time.

- The RPSys uses a set of proven, modern architectural patterns:
  - Saga Pattern, where operations are broken into local transactions with durable checkpoints, enabling safe re-entrant recovery with strong guarantees against duplication or inconsistent state;
  - Idempotent and check-pointed workflows, where every operation step creates a recovery point, allowing:
    - restart from last valid state
    - no duplicate outbound messages
    - no business-rule violations

- consistency across complex workflows;

- Change Feed–Driven Orchestration, where Cosmos DB change feed automatically triggers recovery when items become stalled, ensuring fast, reactive fault handling.

  This combination is extremely robust and aligns with best practices for large-scale distributed systems.

- The system is composed of three independent but cooperating components (Recovery Point Ledger, Recovery Point Orchestrator, RPS), each highly cohesive and loosely coupled.
  This makes the architecture:

  - extendable
  - testable
  - replaceable component-by-component
  - suitable for supporting new REC modifications and new market participant workflows.

  The Recovery Point Service is injected as a shared library, while the Ledger and Orchestrator remain independent services. This is an architectural decision which means the overall CSS balances its core logic (Ledger and Orchestrator) ensuring independent deployments, fault management and scaling, whilst embedding the RPO into other applications, ensuring core functionality remains in-tact irrespective if RPSys incurs an outage.

- The proposed solution addresses shortcomings identified during BCDR events and introduces mechanisms that ensure robustness under failure:

  - Automated detection and replay of stalled operations;
  - Ability to recover from partial failures or missing blob data;
  - Glide-path for safe startup after region failovers;
  - Fail-safe continuation of CSS even if RPSys is temporarily unavailable; and
  - Implementing an automated, programmatic, and organised process to manage messages that cannot be delivered or processed, rather than relying on manual, ad-hoc cleanup. This provides an operational continuity model that was previously not possible.

- The architecture uses horizontally scalable services:

- Cosmos DB auto-scaling, partitioning strategies, and multi-region replication
- Service Bus throughput scaling via Messaging Units

Performance modelling and K6 load testing will validate scalability under peak-of-peak future conditions, with fallback strategies (e.g., fire-and-forget write mode) already planned if volumes exceed synchronous-write limits.

- The system adheres to strict regulatory and compliance standards:
  - Encryption in transit and at rest
  - RBAC and Managed Identities for all access
  - GDPR-aligned data minimisation and retention policies
  - Full audit logs for all actions (ledger writes, orchestrations, recoveries)
  - Governance through Azure Policy and Defender for Cloud ensuring alignment with corporate and REC standards

  This ensures the solution remains compliant with evolving industry and security requirements.

- The design provides industry-leading observability:
  - Real-time dashboards using Power BI & Synapse (trends, stall rates, durations)
  - Azure Monitor logs and telemetry for every recovery point change
  - Recovery-specific alerts and incident integration with Zendesk and ServiceNow
  - Correlation-ID driven tracing for full end-to-end visibility

  This makes the system easier to operate, debug, audit, and improve over time.

- The document explicitly outlines forward-looking enhancements:
  - ML-based stall prediction
  - AI-enhanced triage and automated ticket enrichment
  - Short-term remediation engine for unresolved stalls

  This demonstrates the architecture is flexible enough to incorporate machine learning, automation, and upcoming REC changes.

- The design:
  - does not change existing business processes
  - allows CSS operations to continue even if RPS fails

- reuses existing storage patterns
- limits refactoring to controlled points in the Operations layer
- introduces fail-safes to avoid breaking existing SLAs

This reduces risk during implementation and provides a smooth migration path.

Final Summary

The RPSys is **robust and future-proof** because it is:

- built on resilient Azure-native infrastructure
- architected with modern distributed systems design patterns
- modular, scalable, secure, and highly observable
- capable of automated recovery from partial failures and regional outages
- aligned with existing and future REC requirements
- ready for future enhancements such as AI/ML
- engineered for operational continuity even in worst-case scenarios

The resulting system meaningfully enhances CSS resilience, implements automated procedures should outages occur and minimises the need for manual intervention, and provides a platform that will remain effective and adaptable for years to come.

6. BUSINESS CASE FOR IMPLEMENTING R0096

The R0096 Solution introduces a modern, resilient recovery pattern across all CSS operations. There is a clear, multi-dimensional business case for implementation that covers risk reduction, regulatory compliance, cost avoidance, service stability, and strategic value.

1. Significant Reduction in Operational and Industry-Wide Risk

CSS powers the national switching process. Any stalls or message loss have real industry impact. The design confirms the risk scenarios:

- Operations can stall due to BCDR events, dependency failures, or Azure storage replication delays.
- Lost or delayed messages can create inconsistent business states (e.g., Registrations without corresponding notifications).

The financial and regulatory risk across Suppliers, Networks, and Consumers makes state consistency and recoverability non-negotiable.

RPSys provides full end-to-end state resilience:

- Every operation is checkpointed via the Recovery Point Ledger (Cosmos DB).
- The Orchestrator automatically detects, requeues, and recovers stalled operations.
- Outbound messages are protected from duplication, loss, and reprocessing.

This reduces the likelihood of industry-impacting incidents from “probable” to “highly improbable”.

2. Implementing R0096 has a tangible economic benefit to Industry (Cost vs Benefit analysis)

In Ofgem’s Switching Programme outline business case Impact Assessment and Consultation, it quantified harm to Consumers for a failed or delayed Switch with a value of £30 compensation. This is issued to Consumers under the Guaranteed Standards of Performance (GSOP) scheme. In today’s world, the value for this GSOP compensation is £40.

The original Switching Programme Outline Business Case assessed against the net monetised Consumer benefits over an 18-year period (3 years initial DBT and +15 years of ongoing operation of the CSS).

If we were to assess these costs in today’s world against the original Consumer benefits within the business case, it would show that there is a current net benefit of £3.5m-4m through reduced industry costs.

Should R0096 not be implemented, the CSS would be left exposed to potential subsequent major failures, leading to potential widespread failed and/or delayed Switches. If these were to be of a similar magnitude to the P1 incident in 2023, where ~200,000 Switches were delayed/ failed, based upon the current GSOP compensation payment it could result in a cost to industry of approximately **£8m**.

It should be noted that whilst the costs used here are approximate valuations, they do display the significant economic benefit that R0096 could bring to industry. R0096 not only provides an insurance against the economic impact but also ensures that the downstream impacts of the outages are mitigated. This ensures that the Consumer is not disrupted during their Switching experience.

Further costs are known to be attributed to the resolution of the P1 incident in 2023 relating to impacted organisations' manual intervention and staff FTE costs, but these are not fully quantifiable and therefore have been discounted from the analysis. However, these costs should be considered as increases to the net benefit value.

3. The Cost of Not Doing R0096 Is Higher

Recovering from failures today is manual, slow, and expensive.

Without R0096:

- There is potential for delayed/ failed Switches to occur without any preventative or monitoring mechanisms in place to identify when it has transpired;
- Message regeneration requires deep engineering intervention and manual oversight;
- Stalled operations may cause industry data misalignment;
- Suppliers raise incidents, which require DCC operational effort and may require further effort from CSS user to resend messages;
- Manual replay decisions raise regulatory exposure; and
- Prolonged outages risk SLA breaches and Ofgem escalation.

The proposed solution automates recovery, removing the need for:

- Bespoke replay scripts;
- Incident-triggered batch interventions; and
- Manual triage of inconsistent market states.

The R0096 Design Document explicitly states:

"Failure of the Recovery Point System will not impact Registrations", meaning CSS remains stable even if RPSys is degraded.

This reduction in operational overhead directly reduces DCC and industry support costs.

4. Strengthens Reliability and Performance of the CSS

CSS must meet strict reliability and performance targets. The R0096 Solution Architecture Design Document outlines:

- Availability targets above 99.9%
- Recovery Point Orchestrator: detect & resume a stalled operation within 5 minutes, a reduction from 15 minutes, as is currently in the CSS Service Definition for Registration Service during a BCDR Event.

The current architecture cannot guarantee consistent recovery, especially under multi-region failovers.

With RPSys:

- Every step is idempotent, traceable, and recoverable.
- Outliers in latency or failures are caught and corrected automatically.
- Stalls become rare, short-lived, and observable.

This reduces risk and strengthens the reliability of the CSS infrastructure.

5. Future-Proofed Architecture Lowers Long-Term Total Cost of Ownership

The system uses modern Azure-native, auto-scaling, serverless components:

- Cosmos DB (multi-write, analytical store)
- Service Bus Premium with Geo-DR
- Azure Functions for event-driven orchestration

These services:

- Automatically scale with industry growth;
- Require minimal infrastructure management;
- Reduce future development costs;
- Allow easy extension to new workflows or REC changes; and
- Enable future ML/AI enhancements already envisioned in the document.

Investing now avoids multiplying architectural debt and future expensive refactoring.

6. Dramatically Improves Observability, Reducing Time-to-Diagnose and Time-to-Recover

The system introduces:

- Full recovery-point history for every operation
- Real-time dashboards via Power BI + Synapse

- Change Feed event-driven orchestration
- End-to-end correlation IDs
- Incident integration with Zendesk and ServiceNow

This replaces a previously opaque, difficult-to-trace system.

Faster problem identification means fewer escalations, fewer expensive outages, and quicker service recovery.

7. Supports Market Confidence and Protects the Reputation of the Central Switching Service

Reliable switching is core to Consumer trust in the retail energy market.

Benefits delivered include:

- Protects Market Participants from inconsistent state;
- Prevents duplicate or missing notifications;
- Ensures continuity during outages;
- Reduces incorrect rejections or duplicate Participant submissions; and
- Provides predictable behaviour after BCDR events.

This ensures the CSS remains a high-trust, high-confidence platform.

8. Extremely Favourable Risk-to-Cost Ratio

Costs are predictable and manageable. Azure services scale with usage and are already part of the CSS environment.

Risks mitigated include:

- Industry data corruption
- Business rule breaches
- Manual recovery costs
- Multi-party incident investigations
- Regulatory breaches
- BCDR recovery failures
- Large-scale incident costs (including SLA penalties, reputational damage)

The Design Document stresses that Replication delays, missing messages, and incomplete workflows are real and recurring risks, not theoretical ones. The potential cost of inaction is substantially greater than the cost of implementation.

9. It Directly Addresses a Known and Proven System Weakness

BCDR failures in July 2023 showed that CSS can lose dependent messages during replication lag. The design document states that during the July 2023 event:

- "There is a risk that dependent message files may not be fully replicated to the recovery site",
- Leading to missing notifications, incomplete workflows, and manual reconstruction requirements.

These failures exposed a systemic risk affecting:

- Market Participants;
- DCC's SLA performance;
- Industry trust; and
- Inefficient and costly manual intervention.

R0096 directly resolves the root cause of the 2023 P1 incident, ensuring that all operations can restart safely from a known, consistent point, even after a system incident or regional outage. This is strong evidence of a "burning platform" that R0096 remediates.

Conclusion: A Strong, Evidence-Led Business Case

Implementing R0096 brings a wide variety of benefits to the CSS:

- Fixes a known structural weakness;
- Prevents recurrence of 2023-style BCDR failures;
- Materially reduces operational, regulatory, and financial risk;
- Delivers automated, reliable recovery where none exists today;
- Enhances performance and SLA compliance;
- Provides industry-leading observability and auditability;
- Lowers long-term support and refactoring costs;
- Aligns with future REC and digitalisation requirements; and
- Stabilises the switching ecosystem for the entire market.

These benefits combine to mean that R0096 is a robust and worthwhile solution. R0096 is therefore a solution which:

a. Brings several improvements to the wider CSS system, making it more resilient and reliable, and introduces functionality for all events based driven messaging within its infrastructure;
b. Addresses the issues that were seen in the P1 incident of summer 2023; and
c. Provides value for money for industry by mitigating the downstream impacts of another major outage incident.

R0096 is not merely an improvement. It is a strategic resilience investment that protects the CSS, DCC, and the wider energy industry and end Consumers from high-impact operational risk.

7. HOW WOULD R0096 HAVE HELPED WITH THE P1 INCIDENT?

How many incidents within the P1 would R0096 have stopped?

CSS does not currently categorise incidents in a way that directly aligns with R0096 functionality, so it is difficult to provide an exact count.

Outside of the P1 incident, further instances of 'stalled' messages which currently require manual intervention have been identified since go-live, and can be quantified as below:

- Since go-live, **98 standard changes** have been implemented within the CSS to apply data fixes for stalled Switches across various states.
- Each of these 98 changes for data fixes is rectifying multiple Switches, meaning that the number of impacted Switches is in the multiple hundreds at least (this refers to Switches impacted as opposed to messages not going out).
- Within the context of the R0096 solution, a message can be defined as 'stalled', 'corrupted' or 'lost'. It has been quantified by the CSS Provider that, in line with appropriate activities for incident management, problem management and overall resolution, the cost associated is £1000 per message, however this is proportional to the number of messages impacted by the incident and the resultant issue magnitude.

Why would R0096 have mitigated the impact of the P1 incident?

The technical design of R0096 explains the mitigation approach. In summary:

- The P1 occurred because a Switch did not progress from *Pending/Confirmed* to *Secured Active* at gate closure, with the required messages not present in the queue.
- R0096 introduces a **self-healing mechanism** that breaks down transactions (e.g., a switch) into logical checkpoints (such as state changes or log entries).
- If a transaction fails to reach the next checkpoint within the expected timeframe, the system detects this immediately, rolls back to the last successful checkpoint, and **fixes forward in real time** by generating the missing messages and sending them to Parties as soon as technically possible.
- This proactive approach acts as an **insurance policy against failed processes**, improving resilience and enabling rapid recovery in the event of technical or infrastructure failures.

8. IMPORTANCE TO INDUSTRY

During the Party IA, this solution received two positive responses from DNOs, whilst the GRDA raised concerns relating to clarifications around the technical solution and the costs of implementation and delivery.

At the consultation stage, two DNOs expressed their support for the solution; one Supplier expressed their support for the solution but questioned its high cost to industry; and one Supplier rejected the solution.

As outlined above, the TDA has endorsed the solution under R0096 as strategic resilience investment into the CSS, delivering much-needed fixes to known structural weakness, and provides long-term benefits to the wider energy industry and ultimately Consumers. RECCo are also in favour that a solution within the CSS is in place to improve the CSS's resilience, whilst also mitigating against any future instances similar to the P1 incident of summer 2023.