SanchoNet Disaster Recovery Test Report

Scenario 2: Complete Block Production Halt

Prepared by:
Christian Taylor
Head of Open Source Office, Intersect
&
Johnny Kelly
Seat on TSC and OSC, Intersect
Tech Janitor
&
Mike Hornan
SPO of ABLE stake pool and CEO of Ablevision Network

Date:
Oct 29, 2025

Organization:
Security Council & SanchoNet CIP 135 Scenario 2 Testing Team
Intersect Member Based Organization
Cardano Ecosystem

Review Process	Approval
1st Pass: Johnny Kelly	Approved
2nd Pass: Mike Hornan	Approved
3rd Pass: Security Council	Approved

INTERSECT™

Executive Summary

The SanchoNet team conducted a full-scale disaster recovery exercise to test Scenario 2 of the Disaster Recovery CIP 135, which simulates a total halt in block production. The objective was to validate Cardano's ability to recover from an extended outage where no new blocks can be added to the chain.

Over a 12-hour test window—equivalent to more than 36 hours on mainnet—all block production on SanchoNet was intentionally stopped. The recovery process demonstrated that while the current CIP outlines an impractical methodology involving clock manipulation and 10× block production speed, recovery was achievable using an alternative tool-based approach.

The DB Synthesizer Tool was used to regenerate sufficient empty blocks to rebuild chain density and allow normal block propagation to resume. The network fully recovered from the outage, confirming that the DB Synthesizer approach is a viable and effective method for restoring chain continuity.

Key findings include:

- The current CIP methodology is not practical in its prescribed form.
- The DB Synthesizer Tool should become the preferred mechanism for recovery.
- A new feature is recommended to enable remote polling of SPO keys (KES, Op Cert, VRF) for multi-operator recovery without compromising key security.
- Further testing should validate whether chain truncation is necessary and determine the minimum delegation percentage required for recovery on mainnet.

The exercise successfully restored SanchoNet operations and produced valuable insights that will inform a **recommended CIP revision** and future improvements to recovery tooling.

Test Overview

Scenario: CIP 135 Scenario 2 — Total Block Production Halt
Objective: Validate network recovery procedures following complete block cessation.
Duration: 12 hours (equivalent to 36 hours on mainnet)
Test Environment: SanchoNet test network
Lead Participants: Mike Hornan, Johnny Kelly, and five participating SPOs

Procedure

The test was initiated by Mike Hornan, who reduced the number of active block-producing nodes to five SPOs. These SPOs were instructed to restart their block producers without KES Keys or Operational Certificates (Op Certs), resulting in a total network stall.

After 12 hours, the KES Keys and Op Certs were restored, confirming that the chain was fully halted and unable to accept new blocks. This validated the initial failure condition required by Scenario 2.

Recovery Process

A custom topology.json file was created so the five SPOs could only peer with each other, forming an isolated recovery cluster. Each SPO then truncated their chain databases (both block producers and relays) to several epochs prior to the block halt.
(Note: This truncation step may not be required and will be retested in future simulations.)

According to the existing CIP, SPOs should restart with:

- A manually adjusted wall clock set to a past timestamp, and
- Block production speed increased to 10× normal rate.

However, these steps were not feasible due to the lack of any available tooling or documented process to manipulate system clocks or modify block speeds within Cardano Node software.

Alternative Recovery Method: DB Synthesizer Tool

Given the impracticality of the CIP method, the team employed the DB Synthesizer Tool to regenerate blocks and recover the chain.

This tool allows block padding—creating synthetic blocks—to rebuild the chain tip without running live Cardano nodes. While effective, the DB Synthesizer currently requires all KES Keys, Op Certs, and VRF Keys to be locally available, limiting its scalability and security for mainnet use.

Proposed Feature Enhancement

A feature request was raised for the tool to:

- Remotely poll key data inputs from participating SPOs.
- Allow distributed collaboration without requiring key transfer.
- Preserve key privacy and operator autonomy during coordinated recovery efforts.

Execution Details

For this test, only one SPO's key set (Ticker: INTRT) was used to produce the necessary empty blocks. Because INTRT held approximately 20% of SanchoNet's delegated stake, this was sufficient to generate the required chain density for synchronization.

The DB Synthesizer produced a continuous chain of empty blocks, which the other four SPOs detected and propagated through their isolated topology. Once the expected slot number and tip were reached, all SPOs synchronized, the isolation topology was removed, and normal network operations resumed.

Other SanchoNet participants successfully resynced either by truncating their databases or by performing a full resync from genesis.

Results

- **Successful Recovery:** SanchoNet fully recovered from more than 12 hours of zero block production.
- **Validation:** The DB Synthesizer proved capable of restoring the chain to an operational state.
- **Key Limitation Identified:** The current requirement for centralized key handling limits mainnet feasibility.
- **Next Steps:** Additional tests will validate truncation necessity and multi-SPO collaboration parameters.

Key Findings and Recommendations

Area	Observation	Recommendation
CIP Methodology	Wall clock and 10× block rate changes are impractical.	Revise CIP to reflect realistic recovery tooling.
Tooling	DB Synthesizer successfully restored the	Establish it as the primary recovery mechanism.

	chain.	
Security	Current process requires key sharing.	Implement remote key polling to protect private data.
Scalability	Recovery succeeded with 20% stake delegation.	Define a minimum stake threshold for mainnet recovery scenarios.
Process Efficiency	Truncation may not be required.	Conduct follow-up tests to confirm.

Conclusion

The SanchoNet fire drill successfully validated that a total block production halt can be recovered through a tool-based recovery approach. The current CIP procedure is operationally infeasible and should be updated to reflect modern recovery practices.

It is the consensus of the Scenario 2 test participants that:

> “The Disaster Recovery CIP should be revised to leverage the DB Synthesizer Tool as the core recovery mechanism, eliminating the need for wall clock manipulation or 10× node operation speeds.”

Future testing will focus on refining the process, improving tooling, and ensuring that the recovery pathway is secure, decentralized, and scalable for potential mainnet use.