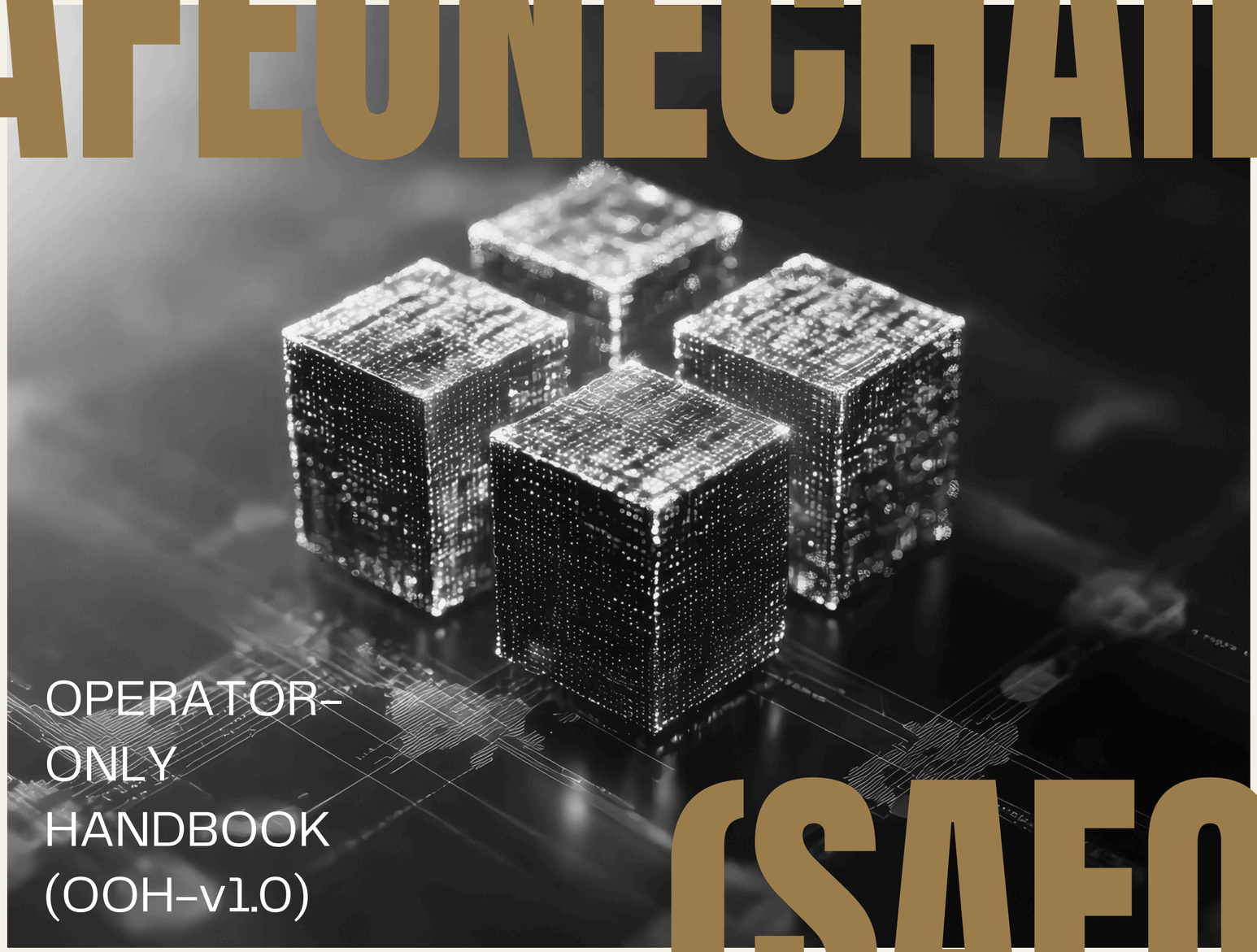
SAFEONECHAIN (SAFO)

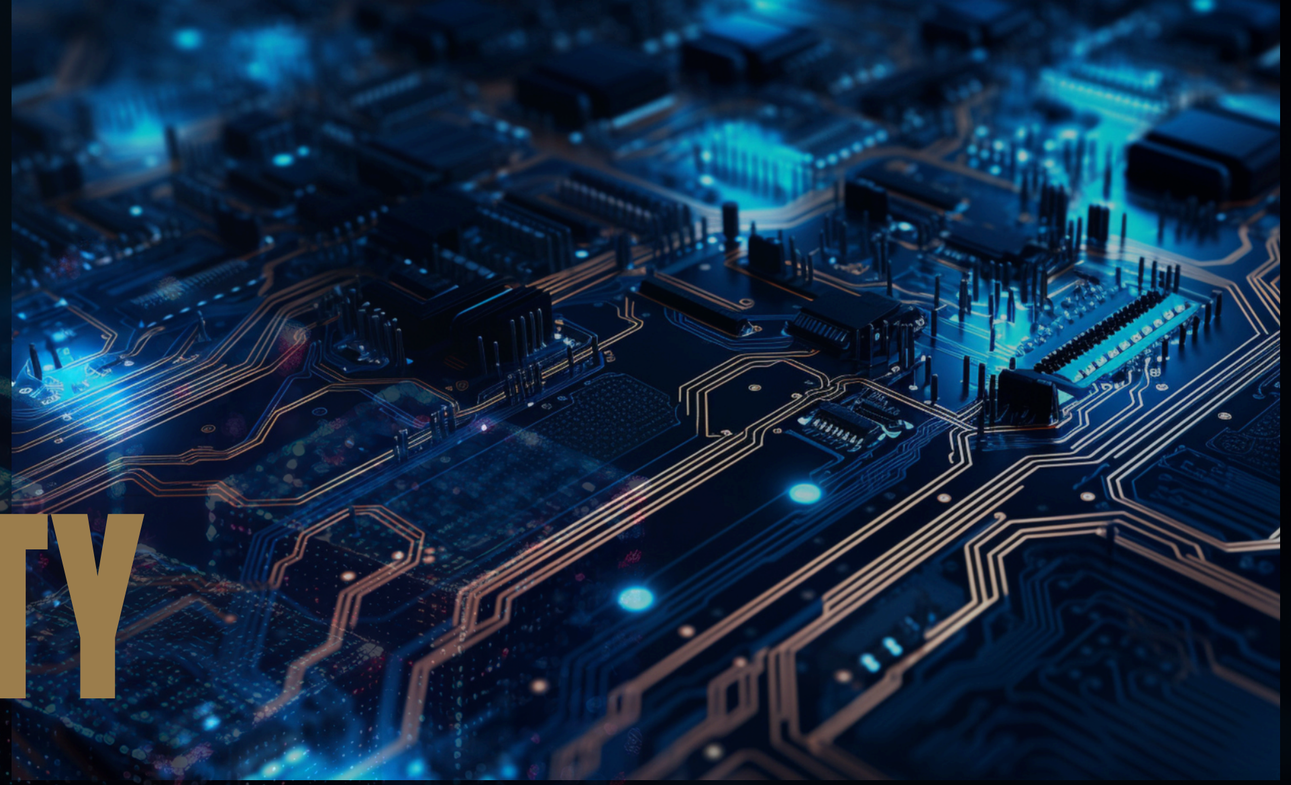


OPERATOR-ONLY HANDBOOK (OOH-v1.0)

SAFO

Status: Canonical Operational ExtractSource of Authority: MPF-v1.0 + DPS-v1.0Code Status: Code Freeze v1.0Audience:Validator Operators, Infrastructure Operators, NOC / SRE Teams, Compliance Ops

SCOPE & OPERATOR RESPONSIBILITY



This document defines operational obligations only.

OPERATORS ARE RESPONSIBLE FOR:

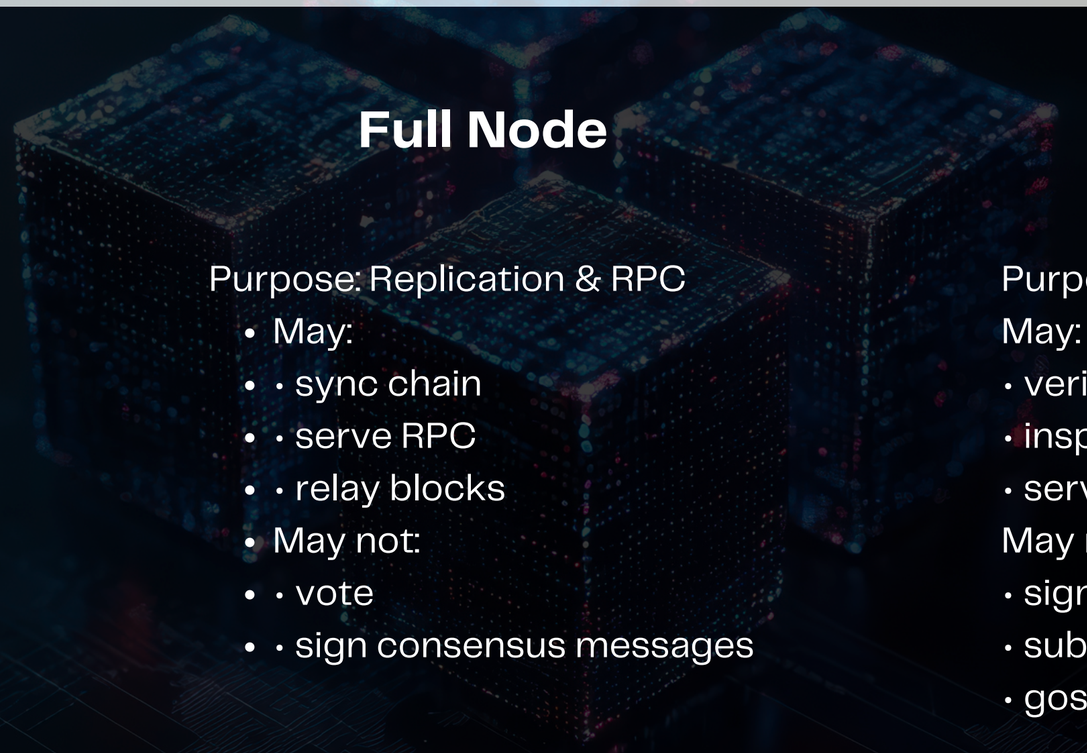
- availability
- key security
- correct node behavior
- incident response

audit cooperation

OPERATORS ARE NOT AUTHORIZED TO:

- change protocol rules
- override finality
- bypass governance
- apply sanctions

Node Roles & Allowed Actions



Validator Node

Purpose: Participate in consensus

May:

- propose blocks
- prevote / precommit
- submit evidence

May not:

- finalize alone
- change validator set
- bypass governance

Full Node

Purpose: Replication & RPC

- May:
- - sync chain
- - serve RPC
- - relay blocks
- May not:
- - vote
- - sign consensus messages

Auditor Node

Purpose: Independent verification

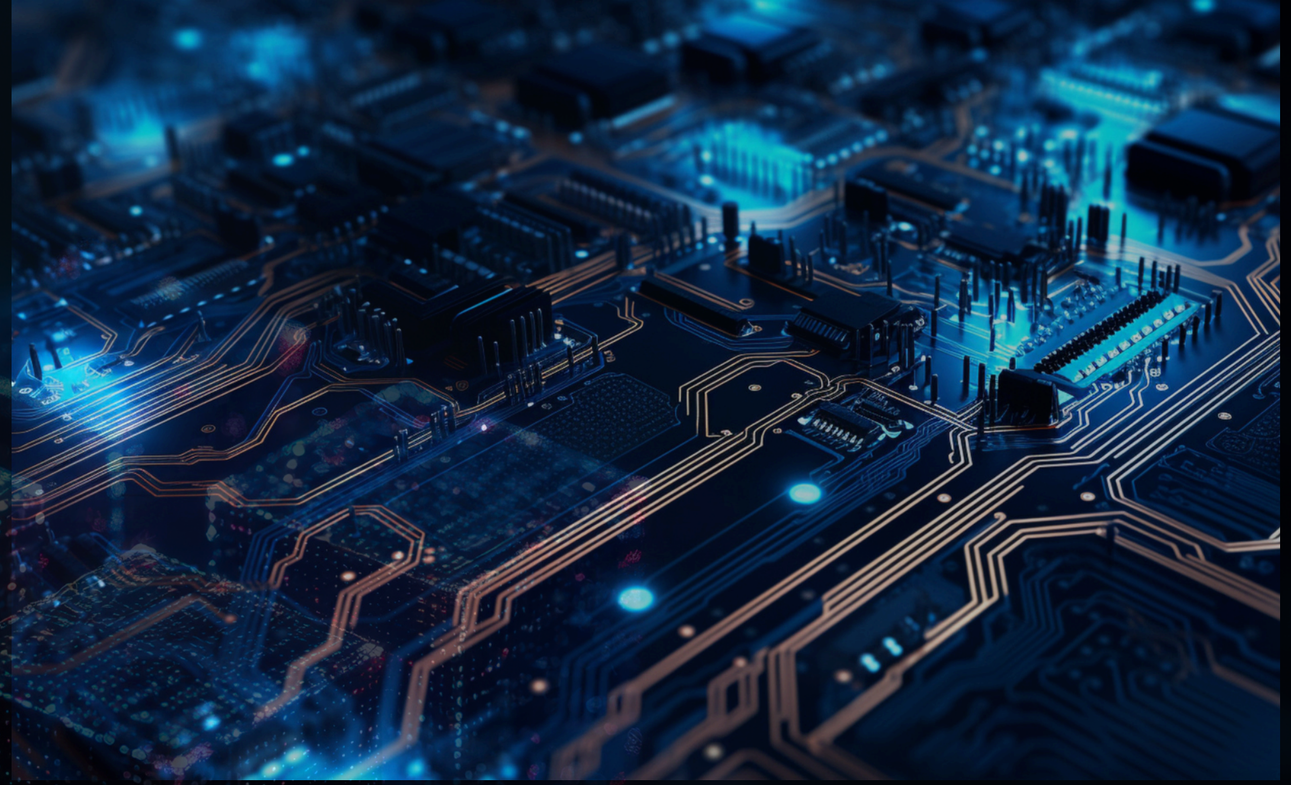
May:

- verify finality proofs
- inspect governance & evidence
- serve read-only RPC

May not:

- sign
- submit transactions
- gossip consensus messages

HARDWARE & INFRASTRUCTURE REQUIREMENTS



MINIMUM (VALIDATOR)

- CPU: 8 cores
- RAM: 32 GB
- Storage: NVMe SSD (≥ 1 TB)
- Network: ≥ 1 Gbps, redundant uplinks

STRONG RECOMMENDATIONS

- Dedicated HSM or remote signer
- Isolated signing environment
- Separate consensus & RPC machines
- Geographically redundant backups

Key Management (CRITICAL)

Validator Keys

- Keys must never reside on the node filesystem
- Use:
  - HSM
  - remote signer
  - air-gapped key service

Key Rotation

- Rotation is allowed
- Rotation must be approved via governance
- Rotation events are on-chain

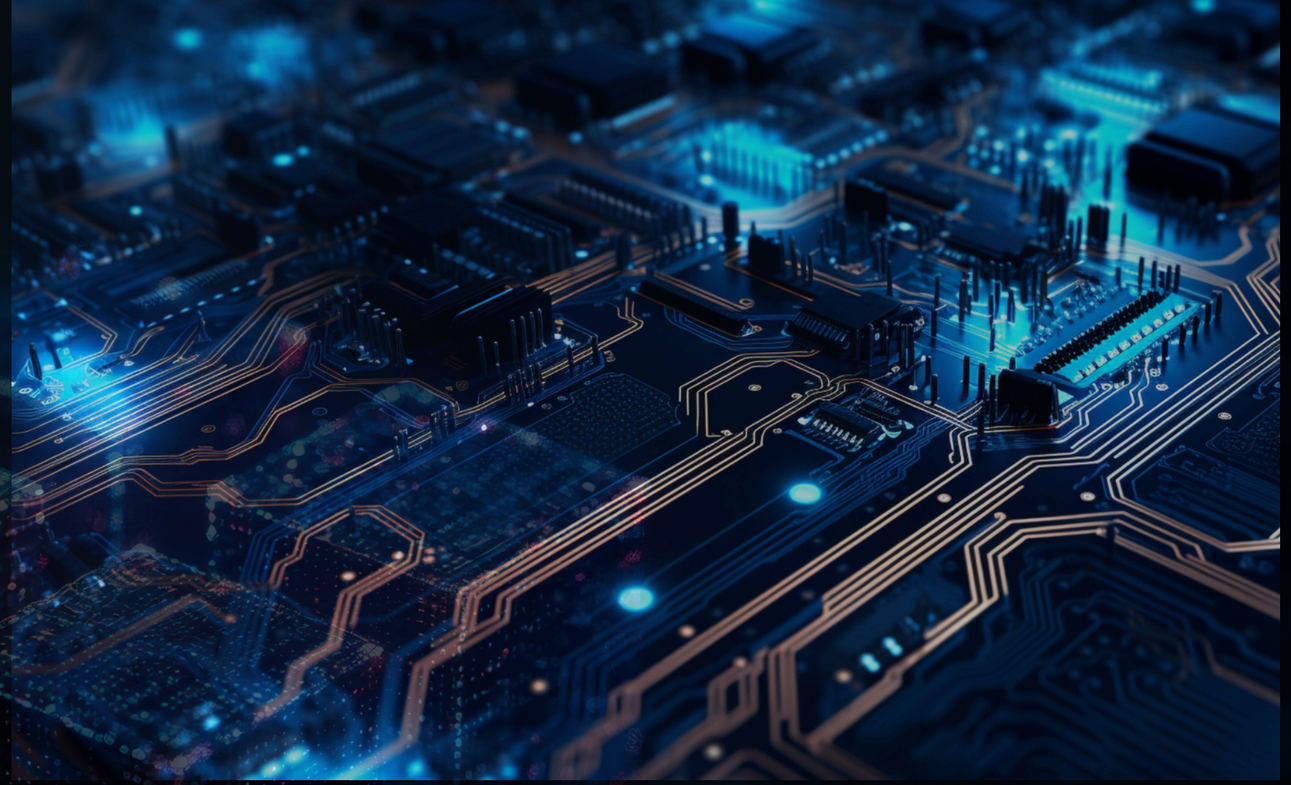
Key Compromise

If compromise is suspected:

1. Immediately stop signing
2. Notify governance
3. Prepare rotation or pause request

Never attempt silent recovery.

NODE CONFIGURATION (OPERATIONAL)



ROLE CONFIGURATION

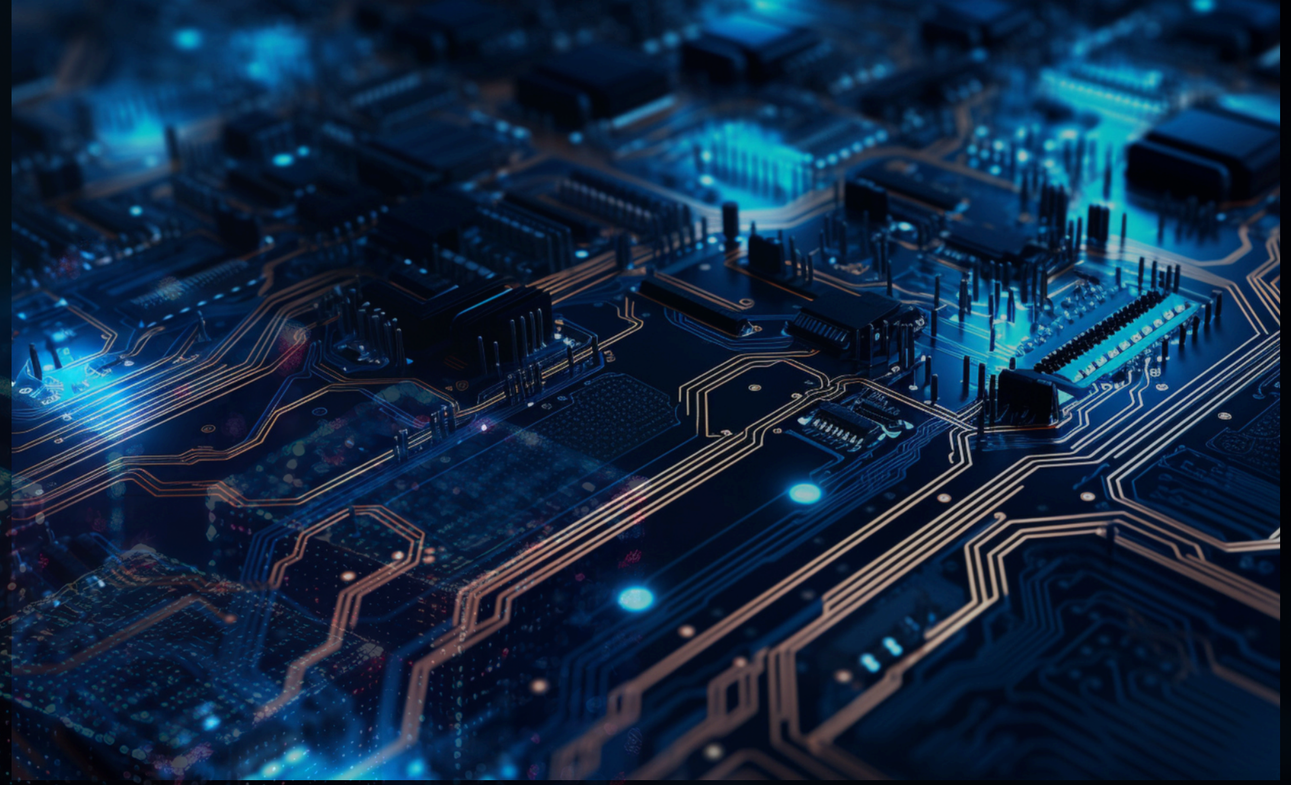
```
[node]
role = "validator" # validator | full |
auditor
rpc_enabled = true
p2p_enabled = true
```

AUDITOR MODE

```
[node]
role = "auditor"
signing_disabled = true
```

Auditor nodes must not have signing capability compiled in.

NETWORKING & CONNECTIVITY



PEER ADMISSION

- Only pre-authorized peers may connect
- No peer discovery

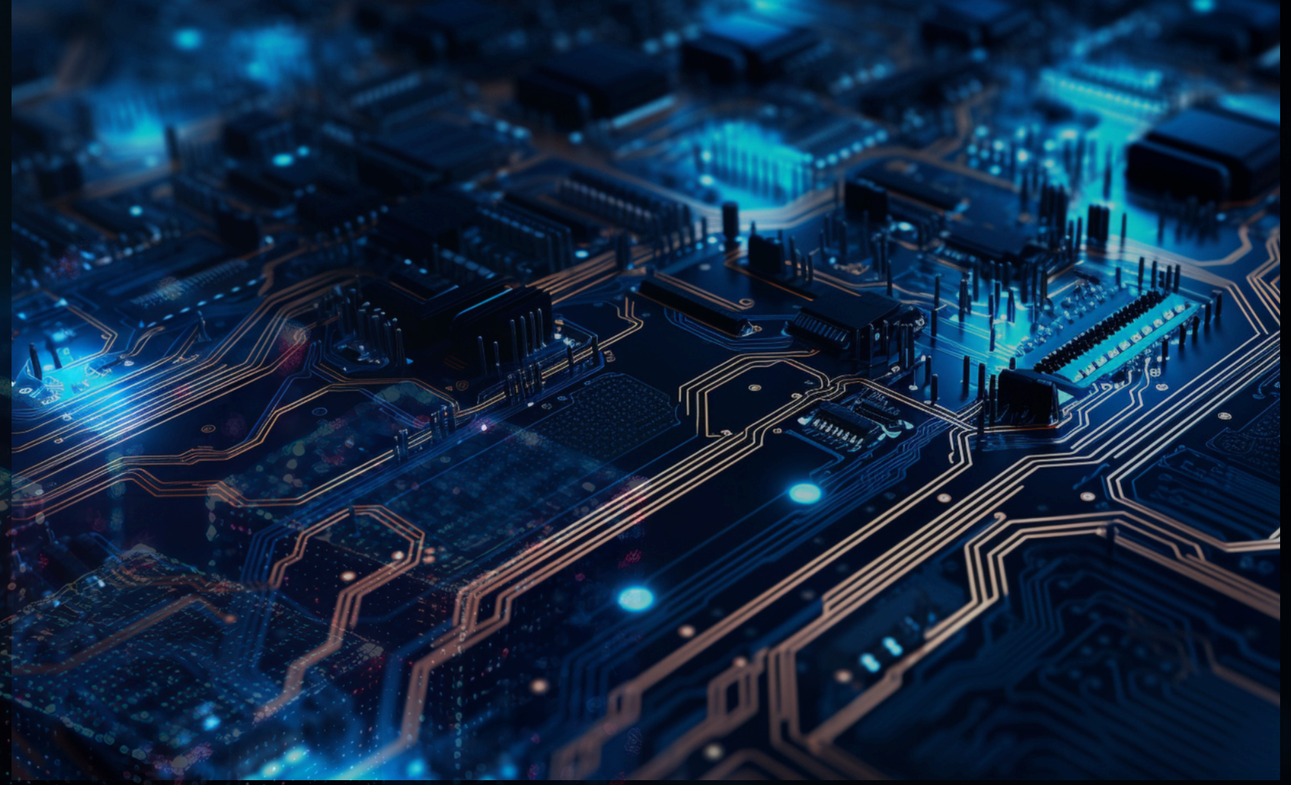
All connections authenticated

RATE LIMITS

Operators must ensure:

- inbound rate limits enabled
- malformed messages drop immediately
- logging enabled for disconnects

MONITORING & ALERTS



MANDATORY METRICS

Operators must monitor:

- block height progression
- finality latency
- missed proposals
- missed votes
- peer count
- signer availability

ALERT CONDITIONS

Immediate alerts on:

- signer unreachable
- double-sign detection
- failure to finalize
- unexpected peer disconnects
- disk saturation

CONSENSUS SAFETY RULES (OPERATOR-RELEVANT)

Operators must ensure:

- only one signer instance per validator key
- no parallel signing processes
- no backup node signs simultaneously

Running two signers with the same key = slash-level offense (via governance).

Incident Response Playbooks

Validator Downtime

1. Confirm local issue
2. Do not restart signer blindly
3. Notify governance if downtime > threshold
4. Restore service carefully

Network Partition

- Do not force reconnection
- Do not override safety checks
- Wait for quorum-safe recovery

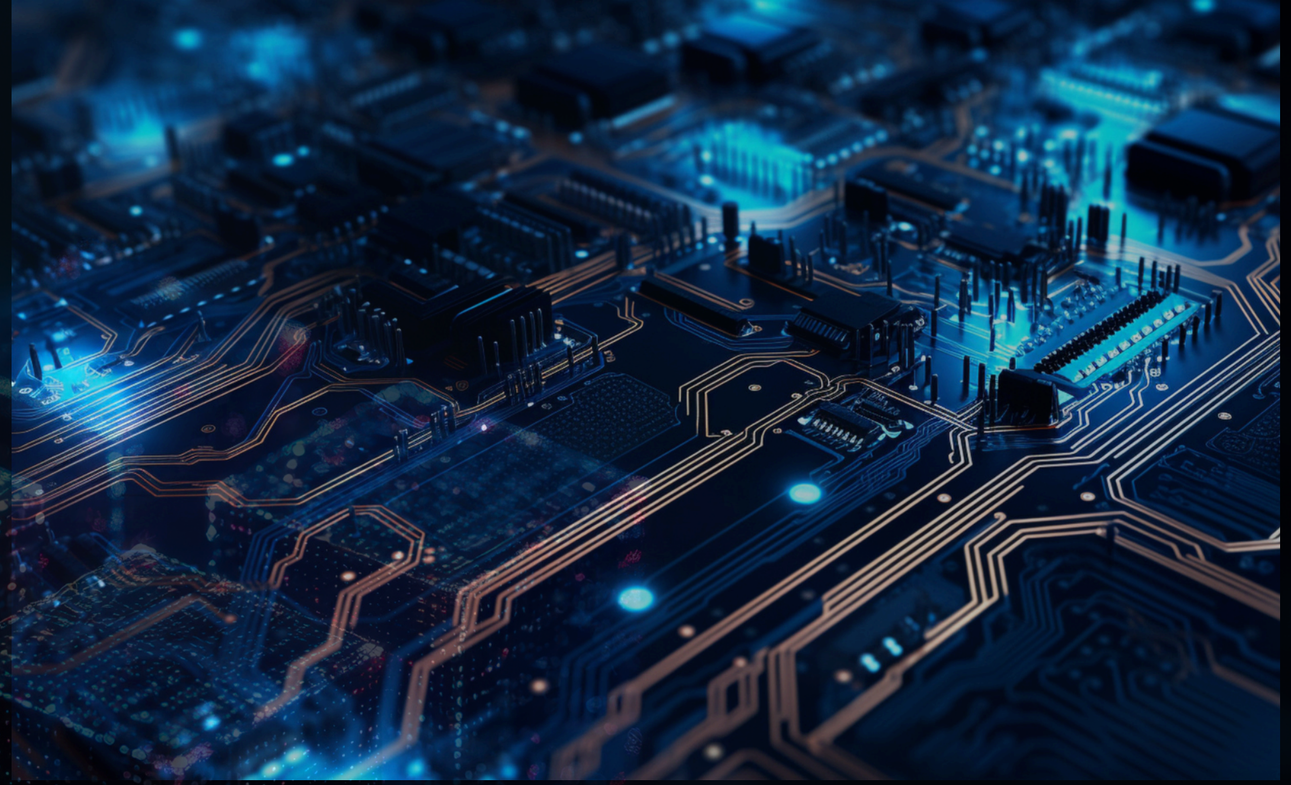
Safety > liveness.

Double-Sign Detection

If detected locally:

1. Stop signer immediately
2. Preserve logs
3. Notify governance
4. Cooperate with evidence submission

SOFTWARE UPDATES & MAINTENANCE



UPGRADE POLICY

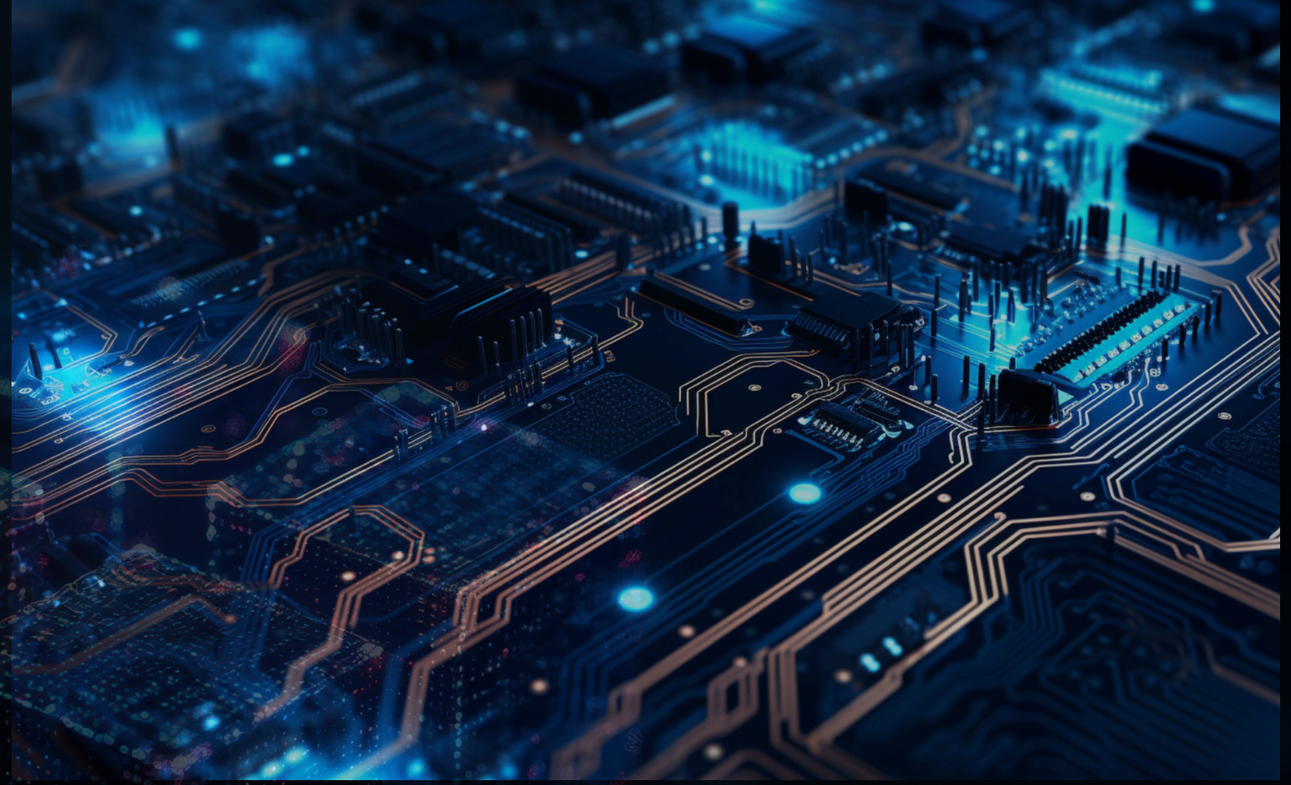
- All upgrades require governance approval
- Rolling upgrades allowed
- Consensus compatibility mandatory

FORBIDDEN ACTIONS

Operators must never:

- hot-patch consensus logic
- alter quorum rules
- change CommitProof encoding
- modify RPC finality behavior

BACKUPS & RECOVERY



REQUIRED BACKUPS

- blockchain data snapshots
- configuration files
- monitoring configuration

Never back up private signing keys in plaintext.

RECOVERY DRILLS

- Quarterly recovery test required
- Must demonstrate:

o no signing during recovery
o clean state replay
o correct finality continuation

AUDIT COOPERATION

Operators are required to:
- provide logs on request
- reproduce harness scenarios if asked
- run auditor nodes if assigned
- not obstruct investigation

Audit cooperation is not optional.

COMPLIANCE BOUNDARIES

Operators:
- execute protocol rules
- do not interpret governance intent
- do not apply sanctions
- do not reverse transactions

Any deviation is non-compliant operation.

CODE FREEZE V1.0 (OPERATOR IMPACT)

At Code Freeze v1.0:
- consensus behavior is fixed
- operator procedures are fixed
- deviations are detectable

Operators must update procedures only with governance-approved releases.

FINAL OPERATOR STATEMENT

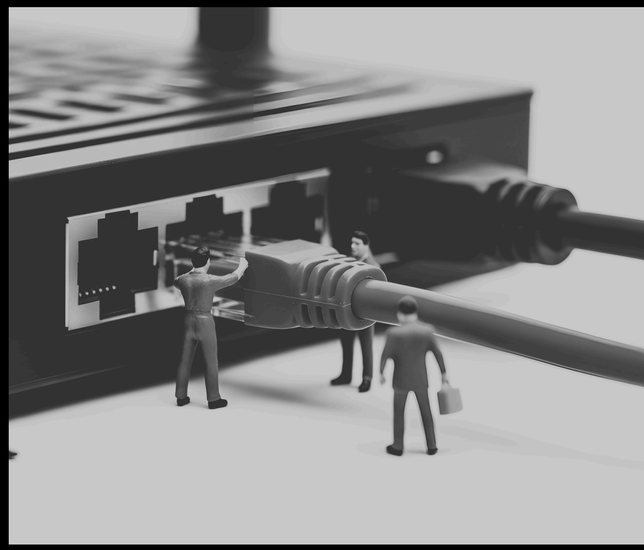
As an operator, we do not control SafeOneChain.We operate it according to fixed rules, under governance oversight, with full accountability.

Document ID: SAFO-OOH-v1.0
Status: FINAL
Derived From: MPF-v1.0 + DPS-v1.0
End of Operator-Only Handbook

X

Medium

CONTACT US



Telegram

safeonechain.com