Stabilytics.fi

Live Infrastructure Audit

Falcon Finance / USDf

Stabilytics.fi

LIVE INFRASTRUCTURE AUDIT

PUBLIC LIA REPORT (UNSOLICITED)

Falcon Finance / USDf

Roles · Signers · Integrations — the live deployment, not the code.

ENGAGEMENT	ISSUED	VERSION	VERIFIED ON-CHAIN
LIA-2026-001	2026-06-02	v1.0	2026-06-02 · Ethereum block 25,229,766 · XDC block 103,572,893 (via Etherscan v2)

FINAL · PILLAR 1 · PILLAR 2 · PILLAR 3

1 CRITICAL · 2 HIGH · 2 MEDIUM · 1 LOW · 1 INFO

CONTENTS

Table of contents

SECTION 01

Executive summary

Stabilytics reviewed the live role, signer and integration configuration of Falcon Finance / USDf across its Ethereum and XDC deployments (the BNB deployment was in scope but not yet verified). The protocol is well-governed at the top: a single 4-of-6 Safe — identical signer set on both chains — is the admin and upgrade authority for the entire estate, with oracle control separated into a distinct 4-of-9 Safe.

The risk concentrates one level below that Safe, in the mint and burn keys. On Ethereum, USDf is minted through a Pre-collateralized Minter whose live execution permission (MINTER_ROLE) is a single externally-owned key; the Safe granted itself that role at deployment and then revoked it. USDf's burn authority is likewise a single EOA, and the token's burn() can target arbitrary holders. We assess the single-EOA mint authority as Critical and the single-EOA burn authority as High.

On the integration side, USDf bridges via Chainlink CCIP (lock on Ethereum, mint on XDC) under the same Safe, but no rate limits are configured on any lane in either direction — a missing circuit breaker on a bridged stablecoin (High). Upgrades, role changes and oracle aggregator swaps all execute immediately, with no timelock (Medium). We recommend, in priority order: move the mint and burn keys off single EOAs, enable CCIP per-lane rate limits, and interpose a timelock on upgrades and oracle changes.

SECTION 02

Engagement context

PROTOCOL Falcon Finance / USDf	ENGAGEMENT ID LIA-2026-001
ENGAGEMENT TYPE Public LIA report (unsolicited)	NETWORKS Ethereum · XDC Network · BNB Smart Chain (not verified)
SOURCE On-chain deployment + public documentation (docs.falcon.finance)	AUDIT DATE June 2026
VERIFIED ON-CHAIN 2026-06-02 · Ethereum block 25,229,766 · XDC block 103,572,893 (via Etherscan v2)	REPORT VERSION v1.0
STATUS FINAL	

SECTION 03

Scope reviewed

Chains in scope	Ethereum · XDC Network · BNB Smart Chain (not verified)

Contracts in scope

CHAIN	CONTRACT	ADDRESS
ETH	USDf	0xFa2B947eEc368f42195f24F36d2aF29f7c24CeC2
ETH	Pre-collateralized Minter	0x3A4F41dac6000a59B79669B9356B5eB71bF4Cc59
ETH	sUSDf	0xc8CF6D7991f15525488b2A83Df53468D682Ba4B0
ETH	sUSDf Staking Rewards Distributor	0x8AF2EFa47efB2095b80D82577c597186Ea2FFFea
ETH	USDf/USD Chainlink Oracle	0xb177857a1799aA5F7fEb5799Fdf12CbE8fdF78B1
ETH	sUSDf/USDf Chainlink Oracle	0xe471bc940AA9831a0AeA21E6F40C1A1236EB4BB3
XDC	USDf	0x8210c0634AB8f273806e4b7866E9Db353773c44B

Authorities audited

DEFAULT_ADMIN, minters, burners, proxy admins / upgrade authority, pausers, reward operators, oracle owners, CCIP token-pool owners.

Out of scope

- Smart-contract code correctness
- Off-chain key custody & signer identity
- BNB Smart Chain deployment (read access pending)
- Collateral composition / yield strategy

SECTION 04

Security posture

CRITICAL — ACTION REQUIRED

Top-level governance is a sound 4-of-6 multisig consistent across chains, but USDf's live mint and burn authority on Ethereum each reduce to a single externally-owned key, and the CCIP bridge runs with no rate limits. Any one of these can threaten the peg until remediated.

SECTION 05

Severity definitions

SEVERITY	DEFINITION
CRITICAL	Active or imminent risk of total or substantial protocol compromise via the authority layer.
HIGH	Material risk of significant loss or operational compromise.
MEDIUM	Notable weakness with realistic exploit paths under specific conditions.
LOW	Hygiene issue or deprecated pattern. No immediate exploit path.
INFORMATIONAL	Observation or note. No risk classification.

SECTION 06

Status definitions

STATUS	MEANING
Open	Identified and verified on-chain; not yet remediated or formally accepted.
Acknowledged	The protocol team has recognised the finding; remediation is pending.
Remediated	Resolved on-chain and re-verified by Stabilytics.
Risk-accepted	The protocol has formally accepted the risk with documented rationale.

SECTION 07

Findings summary

ID	TITLE	SEVERITY	PILLAR	STATUS
P1-001	USDf mint authority on Ethereum terminates at a single externally-owned key	CRITICAL	1	Open
P1-002	USDf BURNER_ROLE is a single EOA with arbitrary-address burn	HIGH	1	Open
P3-001	CCIP cross-chain USDf has no rate limits on any lane	HIGH	3	Open
P1-003	No timelock on upgrades or privileged role changes	MEDIUM	1	Open
P3-002	Own-deployed oracle price source is swappable with no timelock	MEDIUM	3	Open
P1-004	USDf has no global pause / circuit breaker	LOW	1	Informational
INFO-001	Whole-estate governance is one 4-of-6 Safe (consistent, but concentrated)	INFORMATIONAL	1	Informational

SECTION 08

Roles & power distribution

Role inventory

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	USDf	Proxy admin (EIP-1967)	0x3ef1127fdf81b553066dae0faea58785a2aa6e14	contract	INFO
ETH	USDf	Upgrade authority (ProxyAdmin owner)	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
ETH	USDf	Implementation (current)	0x3adf34c09dac24e4baefb1b1df4c2992edc2b789	contract (logic)	INFO
ETH	USDf	DEFAULT_ADMIN_ROLE	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
ETH	USDf	MINTER_ROLE	0x3a4f41dac6000a59b79669b9356b5eb71bf4cc59	contract	HIGH
ETH	USDf	BURNER_ROLE	0x4873f9acff54bdfa97b5f4a7276627dce88c6fdd	EOA	HIGH
ETH	Pre-collateralized Minter	DEFAULT_ADMIN_ROLE	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
ETH	Pre-collateralized Minter	MINTER_ROLE	0x6cbf64be2af1faf2041c34c877eea7dc2c135dd9	EOA	CRITICAL
ETH	sUSDf	Proxy admin (EIP-1967)	0x16a2605c026bfe4f4b7f4471933714d9b2149ace	contract	INFO

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
ETH	sUSDf	Upgrade authority (ProxyAdmin owner)	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
ETH	sUSDf	Implementation (current)	0x0d132bee412e6619a4863aeedad97541bfda3f34	contract (logic)	INFO
ETH	sUSDf	DEFAULT_ADMIN_ROLE	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
ETH	sUSDf	REWARDER_ROLE	0x8af2efa47efb2095b80d82577c597186ea2fffea	contract	LOW
ETH	sUSDf Staking Rewards Distributor	DEFAULT_ADMIN_ROLE	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
ETH	sUSDf Staking Rewards Distributor	PAUSER_ROLE	0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	LOW
ETH	sUSDf Staking Rewards Distributor	OPERATOR_ROLE	0xbced57e512996eee346afa23e3762e8cedf334d8	Safe	LOW
ETH	sUSDf Staking Rewards Distributor	OPERATOR_ROLE	0x482d74fdf4e33773735c2f53a8b5f47af1f5c8aa	EOA	MEDIUM
ETH	sUSDf Staking Rewards Distributor	paused()	false	state	INFO
ETH	USDf/USD Chainlink Oracle	owner	0x21f73d42eb58ba49ddb685dc29d3bf5c0f0373ca	Safe 4-of-9	MEDIUM
ETH	sUSDf/USDf Chainlink Oracle	owner	0x21f73d42eb58ba49ddb685dc29d3bf5c0f0373ca	Safe 4-of-9	MEDIUM

CHAIN	CONTRACT	ROLE	HOLDER	TYPE	RISK
XDC	USDf	DEFAULT_ADMIN_ROLE	0x1ee82b60bf19cb1cc859389e0ea3ded153f16bd7	Safe 4-of-6	MEDIUM
XDC	USDf	MINTER_ROLE	0x33570299e0d73f07c82d005de75de54cf4582fcc	contract	HIGH
XDC	USDf	BURNER_ROLE	0x33570299e0d73f07c82d005de75de54cf4582fcc	contract	HIGH

Cross-chain parity matrix

ROLE	ETH	XDC	BNB	PARITY
DEFAULT_ADMIN_ROLE on USDf	Safe 4-of-6	Safe 4-of-6 (same 6 signers)	—	✓ Parity — Identical admin Safe across chains.
USDf mint authority	Pre-collateralized Minter → single EOA executor	CCIP Burn/Mint pool → 4-of-6 Safe owner	—	× Gap — Mint is operated by a lone EOA on Ethereum; on XDC it is a Safe-owned CCIP pool.
USDf burn authority	Single EOA (0x4873···6fdd)	CCIP Burn/Mint pool	—	× Gap — Arbitrary-address burn key is an EOA on Ethereum.
USDf upgradeability	Transparent proxy (upgradeable, no timelock)	Non-proxy (immutable)	—	⚠ Differs — Token is upgradeable on Ethereum, immutable on XDC.
Pause / circuit breaker on USDf	None (per-address freeze only)	None	—	⚠ Differs — No global pause on the token on either chain.

Parity headline: USDf mint/burn authority is structured very differently per chain: on Ethereum it routes through a single-EOA-operated Pre-collateralized Minter; on XDC through a 4-of-6-Safe-owned CCIP burn/mint pool. The shared protocol admin is one 4-of-6 Safe with an identical signer set on both chains.

SECTION 09

Signer trust analysis

Per-signer profiles

Address	`0x1e482b60bf19cb1cc859389e0ea3ded153f16bd7`
Type	Safe 4-of-6
In multisigs	USDf/sUSDf/Minter/Distributor DEFAULT_ADMIN, USDf+sUSDf upgrade authority, CCIP pool owner (ETH+XDC)
Power weight	Grants/revokes every role across the core estate, upgrades USDf & sUSDf, owns both CCIP token pools.
Attribution	Unattributed (no off-chain identity asserted)
Risk	HIGH

A single 4-of-6 Safe governs the entire core deployment on both chains. The 4-of-6 threshold is reasonable, but the concentration means one multisig compromise (or 4-of-6 collusion) is systemic across roles, upgrades and the bridge.

Address	`0x21f73d42eb58ba49ddb685dc29d3bf5c0f0373ca`
Type	Safe 4-of-9
In multisigs	USDf/USD oracle owner, sUSDf/USDf oracle owner
Power weight	Can propose/confirm a new aggregator (price source) on both Falcon-deployed Chainlink proxy feeds.
Attribution	Unattributed (no off-chain identity asserted)
Risk	MEDIUM

Oracle governance sits in a separate 4-of-9 Safe with a signer set fully disjoint from the protocol-admin Safe — a positive separation of duties. Price-source changes are nonetheless immediate (no timelock).

Address	`0xbced57e512996eee346afa23e3762e8cedf334d8`
Type	Safe (threshold not enumerated)
In multisigs	Distributor OPERATOR_ROLE
Power weight	Operational reward parameters on the staking rewards distributor.
Attribution	Unattributed

Risk	LOW

> One of two OPERATOR_ROLE holders; a multisig. The second operator is an EOA (see findings).

Cross-multisig signer overlap

SIGNER	ADMIN 4-OF-6	ORACLE 4-OF-9	NOTES
`Owner-set intersection`	6 owners	9 owners	Disjoint — no shared signer between the protocol-admin Safe and the oracle Safe. Separation of duties is in place.

SECTION 10

Third-party integrations

Integration inventory

#	INTEGRATION	CHAIN	INSTANCE	CONFIGURATION
1	CCIP Lock/Release token pool	ETH	0xecf61d6faa3b9fae7195af3bc9891450c1733f78	Owner 4-of-6 Safe · 4 lanes (incl. BNB, XDC) · allowlist disabled · rate limits DISABLED on all lanes
2	CCIP Burn/Mint token pool	XDC	0x33570299e0d73f07c82d005de75de54cf4582fcc	Owner 4-of-6 Safe · ETH lane · allowlist disabled · inbound+outbound rate limits DISABLED
3	Upgradeable proxy (Transparent)	ETH	USDf 0xFa2B··· & sUSDf 0xc8CF···	ProxyAdmin owner = 4-of-6 Safe · no timelock
4	Chainlink price proxy (EACAggregatorProxy)	ETH	USDf/USD 0xb177··· & sUSDf/USDf 0xe471···	Owner 4-of-9 Safe · aggregator swappable · no timelock

CCIP token-pool configuration

POOL	CHAIN	TYPE	OWNER	LANES	ALLOWLIST	RATE LIMITS
0xecf6··· 3f78	Ethereum	Lock/Release 1.5.1	Safe 4-of-6	4 (BNB, XDC, +2)	Disabled	Disabled (all lanes)
0x3357··· 2fcc	XDC	Burn/Mint 1.5.1	Safe 4-of-6	1 (Ethereum)	Disabled	Disabled (in & out)

Default-vs-customized

INTEGRATION	DEFAULTS RETAINED?	STATUS	RISK IF DEFAULTS
CCIP per-lane rate limits	Disabled (no cap)	None set	HIGH
CCIP sender allowlist	Disabled (open)	None set	LOW

INTEGRATION	DEFAULTS RETAINED?	STATUS	RISK IF DEFAULTS
Proxy upgrade timelock	None	None set	MEDIUM
Oracle aggregator-change timelock	None	None set	MEDIUM

SECTION 11

Audit findings

CRITICAL (1)

P1-001 USDf mint authority on Ethereum terminates at a single externally-owned key

CRITICAL

Location	Ethereum — Pre-collateralized Minter 0x3A4F···Cc59 (MINTER_ROLE) → USDf 0xFa2B···CeC2 (MINTER_ROLE)
Status	accepted

DESCRIPTION

USDf issuance on Ethereum is gated by MINTER_ROLE, held solely by the Pre-collateralized Minter contract (0x3A4F··· Cc59). The Minter's own operational MINTER_ROLE — the on-chain permission to execute preCollateralizedMint(), which calls USDf.mint() — is held by a single externally-owned account, 0x6cbf64be2af1faf2041c34c877eea7dc2c135dd9 (eth_getCode returns 0x). The 4-of-6 admin Safe held this role at deployment and then revoked it (tx 0x7c1baf39···), leaving the EOA as the only live mint-execution key. Mints are authorised by an off-chain EIP-712 signature over MintParams{collateralRef, recipient, amount, nonce, expiry}; collateralRef is an opaque reference and no collateralisation is verified on-chain.

IMPACT

Compromise of this single key — together with the off-chain signer, whose custody is not verifiable on-chain — permits minting USDf with no on-chain collateral check, directly threatening the peg of a stablecoin with ~1.47B USDf in circulation on Ethereum alone. A single externally-owned mint key on a stablecoin is the exact pattern behind the Resolv incident ($25M).

REPRODUCTION / EVIDENCE

```
getLogs RoleGranted/RoleRevoked on 0x3A4F…Cc59: MINTER_ROLE granted to 0x6cbf…5dd9 (by the Safe)
and revoked from the Safe in tx 0x7c1baf39… → net holder = 0x6cbf…5dd9. eth_getCode(0x6cbf…5dd9)
= 0x (EOA). USDf MINTER_ROLE holder = 0x3A4F…Cc59 (the Minter). Minter ABI exposes
preCollateralizedMint(MintParams,bytes). Verified Ethereum mainnet 2026-06-02.
```

RECOMMENDATION

- Transfer the Minter's MINTER_ROLE from the single EOA to a threshold multisig (⩾ 3-of-5) or an HSM/MPC signer with separation of duties from the EIP-712 signer.
- If an automated hot signer is operationally required, enforce on-chain per-period mint caps and a short timelock on cap changes, so a key compromise cannot mint unbounded supply.
- Verify after change: hasRole(MINTER_ROLE, 0x6cbf···5dd9) == false on 0x3A4F···Cc59.

REFERENCES

Resolv Labs — single-EOA mint authority ($25M)

HIGH (2)

P1-002 USDf BURNER_ROLE is a single EOA with arbitrary-address burn

HIGH

Location	Ethereum — USDf 0xFa2B···CeC2 — BURNER_ROLE 0x4873···6fdd
Status	accepted

DESCRIPTION

USDf exposes burn(address from, uint256 amount), gated by onlyRole(BURNER_ROLE). Verified against the deployed implementation source (0x3adf···b789): the function body is _burn(from, amount) — OpenZeppelin's internal burn, which deducts directly from the target's balance with no allowance or approval check (the only additional guard is a denylist check that reverts if from/to are restricted). The sole BURNER_ROLE holder is an externally-owned account, 0x4873f9acff54bdfa97b5f4a7276627dce88c6fdd (eth_getCode = 0x).

IMPACT

A compromise of this single key allows burning USDf from any non-denylisted holder address without their consent — enabling targeted balance destruction, griefing, and supply manipulation. Concentrated in one EOA, it is a single point of failure parallel to the mint key.

REPRODUCTION / EVIDENCE

```
Deployed impl source (0x3adf…b789): `function burn(address from, uint256 amount) external
onlyRole(BURNER_ROLE) { _burn(from, amount); }`; OZ _burn → _update(from, address(0), amount)
with only an isRestricted[from]/[to] guard, no allowance check. BURNER_ROLE holder (from USDf
RoleGranted logs, no revoke) = 0x4873…6fdd; eth_getCode(0x4873…6fdd)=0x (EOA). Verified Ethereum
mainnet 2026-06-02.
```

RECOMMENDATION

- Move BURNER_ROLE to a multisig, or constrain burn to protocol-owned redemption/treasury addresses only.
- Verify: hasRole(BURNER_ROLE, ···) resolves to a contract/multisig, not an EOA.

REFERENCES

Resolv Labs — single-EOA privileged token authority

P3-001 CCIP cross-chain USDf has no rate limits on any lane

HIGH

Location	Ethereum LockRelease pool 0xecf6···3f78 (4 lanes) & XDC BurnMint pool 0x3357···2fcc (ETH lane)
Status	accepted

DESCRIPTION

USDf bridges via Chainlink CCIP: a LockRelease pool on Ethereum (lock origin) and a BurnMint pool on XDC (mint destination), both owned by the 4-of-6 Safe. Every lane's inbound and outbound rate limiter is disabled (isEnabled=false, capacity=0, rate=0) on both pools, and the sender allowlist is disabled.

IMPACT

Rate limits are the circuit breaker that bounds a bridge-layer failure. With none configured, a CCIP/RMN or pool-level failure that mints on a destination chain has no on-chain cap to contain it, exposing the full bridged supply. Defense-in-depth is absent on a bridged stablecoin.

REPRODUCTION / EVIDENCE

> `typeAndVersion: "LockReleaseTokenPool 1.5.1" (0xecf6…3f78), "BurnMintTokenPool 1.5.1" (0x3357…2fcc). getCurrentInbound/OutboundRateLimiterState for the XDC lane and all four ETH-side lanes return isEnabled=false, capacity=0, rate=0. getAllowListEnabled()=false on both. owner()=0x1e48…6bd7 (4-of-6 Safe) on both. Verified 2026-06-02.`

RECOMMENDATION

- Enable per-lane inbound and outbound rate limits sized to expected legitimate flow on both pools (setChainRateLimiterConfig).
- Re-evaluate whether the sender allowlist should be enabled for the burn/mint lane.
- Reconcile the four advertised ETH-side lanes against the three chains in public docs.

REFERENCES

Chainlink CCIP — token-pool rate limiting
Nomad Bridge — $190M, unbounded bridge minting (rekt)
Wormhole — $325M bridge mint exploit (rekt)

MEDIUM (2)

P1-003 No timelock on upgrades or privileged role changes

MEDIUM

Location	Ethereum — USDf & sUSDf ProxyAdmins (owner 4-of-6 Safe); DEFAULT_ADMIN across all contracts
Status	accepted

DESCRIPTION

USDf and sUSDf are Transparent upgradeable proxies whose ProxyAdmins are owned directly by the 4-of-6 Safe, with no TimelockController in between. All role grants/revocations and implementation upgrades take effect immediately on Safe execution.

IMPACT

A compromised or colluding 4-of-6 Safe can swap the USDf/sUSDf implementation or re-grant mint/burn authority instantly, with no delay window for users or integrators to react or exit.

REPRODUCTION / EVIDENCE

```
EIP-1967 admin slot → ProxyAdmin 0x3ef1…6e14 (USDf) / 0x16a2…9ace (sUSDf); ProxyAdmin.owner() = 0x1e48…6bd7 (Safe 4-of-6). No timelock contract observed in the upgrade path. Verified 2026-06-02.
```

RECOMMENDATION

- Interpose a TimelockController (e.g. 24–48h) between the Safe and the ProxyAdmins / DEFAULT_ADMIN, with the Safe as proposer.
- Publish the timelock address and delay so integrators can monitor pending changes.

REFERENCES

Drift Protocol — multisig social-engineering ($285M scope)

P3-002 Own-deployed oracle price source is swappable with no timelock — MEDIUM

Location	Ethereum — USDf/USD 0xb177…78B1 & sUSDf/USDf 0xe471…4BB3 (EACAggregatorProxy)
Status	accepted

DESCRIPTION

Both Falcon-deployed Chainlink proxy feeds are owned by a 4-of-9 Safe (0x21f7…73ca) that can call proposeAggregator/confirmAggregator to repoint the underlying price source. Changes take effect with no timelock.

IMPACT

These feeds are the published USDf/USD and sUSDf/USDf price sources that integrators and lending markets may consume. The owning Safe can swap the aggregator behind the same address; a malicious or erroneous swap mis-prices USDf at every downstream integrator simultaneously.

REPRODUCTION / EVIDENCE

```
owner() on both proxies = 0x21f7…73ca; getThreshold()=4, getOwners() length 9 → Safe 4-of-9 (signer set disjoint from the admin Safe). aggregator() (USDf/USD) = 0x0558…ef5e. Verified 2026-06-02.
```

RECOMMENDATION

- Timelock aggregator changes on both feeds and publish the governance process.
- Document for integrators that these are protocol-owned proxies, not first-party Chainlink feeds.

REFERENCES

Chainlink — aggregator proxy ownership model

LOW (1)

P1-004 USDf has no global pause / circuit breaker — LOW

Location	Ethereum & XDC — USDf token
Status	accepted

DESCRIPTION

USDf exposes no pause(); paused() reverts. Emergency control is limited to per-address restriction (setRestriction/isRestricted). The staking rewards distributor is pausable (PAUSER_ROLE = 4-of-6 Safe, currently unpaused).

IMPACT

In an incident, the protocol cannot halt all USDf transfers; it can only freeze individual addresses. This is a design trade-off (avoids a single transfer-kill switch) but removes a system-wide circuit breaker.

REPRODUCTION / EVIDENCE

```
eth_call paused() on USDf reverts; implementation ABI has setRestriction/isRestricted and no Pausable. Distributor paused() = false. Verified 2026-06-02.
```

RECOMMENDATION

- Confirm this is intentional; if a circuit breaker is desired, add a guardian-gated pause with a multisig pauser.

INFORMATIONAL (1)

INFO-001 Whole-estate governance is one 4-of-6 Safe (consistent, but concentrated) — INFORMATIONAL

Location	Ethereum & XDC — admin Safe 0x1e48···6bd7
Status	accepted

DESCRIPTION

A single 4-of-6 Safe with an identical six-signer set on Ethereum and XDC is DEFAULT_ADMIN of USDf, sUSDf, the Minter and the Distributor; upgrade authority for USDf and sUSDf; and owner of both CCIP token pools. Oracle governance is a separate, disjoint 4-of-9 Safe.

IMPACT

The cross-chain consistency and the 4-of-6 threshold are positive. The flip side is concentration: this one Safe is the root of authority for the entire estate on both chains, so its compromise is systemic. The single-EOA mint/burn keys (P1-001/P1-002) sit beneath this Safe operationally.

REPRODUCTION / EVIDENCE

```
getOwners()/getThreshold() on 0x1e48…6bd7 = 6 owners / threshold 4 on both Ethereum and XDC (identical owner set). Verified 2026-06-02.
```

RECOMMENDATION

- Consider raising the threshold (e.g. 5-of-8) as TVL grows, and document signer-key custody and geographic/role distribution.

SECTION 12

Centralisation & power concentration

Authority over the entire Falcon estate roots in a single Gnosis Safe (0x1e48···6bd7), a 4-of-6 multisig with an identical six-signer set on both Ethereum and XDC. It is DEFAULT_ADMIN of USDf, sUSDf, the Pre-collateralized Minter and the Rewards Distributor; the upgrade authority (via ProxyAdmin owner) for USDf and sUSDf; and the owner of both CCIP token pools. The 4-of-6 threshold and cross-chain consistency are genuinely good practice — but the concentration means a single multisig compromise, or collusion of four signers, is systemic across roles, upgrades and the bridge simultaneously.

One level below that Safe, day-to-day execution is delegated to single externally-owned keys. USDf's operational mint authority on Ethereum is a lone EOA operating the Pre-collateralized Minter (the Safe granted itself MINTER_ROLE at deployment and then revoked it), and USDf's burn authority is a second lone EOA able to burn from arbitrary holders. These hot keys are the practical attack surface: they do not require multisig approval to act, so their custody — which is off-chain and outside this review — is load-bearing for the peg.

Two mitigating structural choices are worth crediting: oracle control is separated into a distinct 4-of-9 Safe whose signer set does not overlap the protocol-admin Safe (a real separation of duties), and the Minter, Distributor and XDC token are non-upgradeable. The countervailing weakness is the absence of any timelock — upgrades, role changes and oracle aggregator swaps all take effect immediately on multisig execution, leaving no window for users or integrators to react.

SECTION 13

Remediation roadmap

PRIORITY	FINDING	RECOMMENDATION	EFFORT	OWNER
1 (immediate)	P1-001	Replace single-EOA Minter execution key with multisig/MPC + on-chain mint caps	1–2 days	Protocol team
1 (immediate)	P1-002	Move USDf BURNER_ROLE off the EOA; constrain arbitrary-address burn	1 day	Protocol team
2 (this week)	P3-001	Enable per-lane CCIP rate limits on both token pools	1 day	Protocol team
3 (this month)	P1-003	Interpose 24–48h timelock on upgrades and role-admin	2–3 days	Protocol team
3 (this month)	P3-002	Timelock oracle aggregator changes	1–2 days	Protocol team
4 (review)	P1-004	Decide on a system-wide circuit breaker	discussion	Protocol team

SECTION 14

Conclusion

Falcon Finance presents a mature top-level governance posture wrapped around an operational key layer that has not kept pace with it. The multisig design is sound; the single-EOA mint and burn keys, and the unthrottled CCIP bridge, are the gap between a well-governed protocol and a resilient one. None of the headline findings require a redesign — each has a concrete, low-effort remediation.

In priority order: (1) move the Minter's mint-execution key and USDf's burn key off single EOAs onto multisig/MPC with on-chain caps; (2) enable per-lane CCIP rate limits on both token pools; (3) interpose a 24–48h timelock on upgrades, role-admin and oracle aggregator changes. The BNB Smart Chain deployment was in scope but could not be verified in this pass and should be confirmed before this report is treated as complete across all three chains.

SECTION 15

Methodology

Stabilytics performed a Live Infrastructure Audit (LIA) across Pillars 1 (roles & power distribution), 2 (signer trust structure) and 3 (integration configuration) against live on-chain state, not source code. Every privileged role was enumerated from on-chain reads and reconstructed from RoleGranted/RoleRevoked event history; each holder was classified as EOA, Safe (with threshold), or contract from on-chain code and Safe getters.

Proxy and upgrade authority were read directly from EIP-1967 storage slots and ProxyAdmin owners. CCIP integration was characterised from the token pools' typeAndVersion, owner, supported lanes, allowlist and rate-limiter state. Oracle control was read from the EACAggregatorProxy owners.

AI and scanners accelerated enumeration; every finding and severity call was verified by a human Stabilytics engineer, and every Critical/High was independently peer-reviewed before transmission. The tool reports facts; severity and recommendations are human-owned.

All reads were verified on Ethereum mainnet and XDC Network on 2026-06-02. The BNB Smart Chain USDf deployment was in scope but could not be read in this pass and is marked unverified.

SECTION 16

Disclaimer & scope limits

Findings reflect on-chain state at the moment of verification (2026-06-02). Configurations may change after delivery.

This is an unsolicited public report. Stabilytics was not engaged or compensated by Falcon Finance. All findings are based on publicly available on-chain data and public documentation at docs.falcon.finance.

Stabilytics did not perform smart-contract code review, off-chain key-custody assessment, or signer identity attribution. Code-level behaviour of preCollateralizedMint (e.g. signature/collateral logic) was not audited.

The BNB Smart Chain deployment was not verified in this pass; its roles may differ from Ethereum and XDC.

SECTION 17

About Stabilytics

Stabilytics audits the **live deployment** of Web3 protocols — the roles, signers, and third-party integrations that determine who controls a protocol and what happens if that control is compromised. This is the layer between a smart-contract audit (does the code do what it says?) and an OPSEC review (do the people follow safe practices?) — a blind spot that has cost protocols hundreds of millions of dollars.

Engagements are **human-authored and peer-reviewed**; tooling accelerates enumeration but every finding and severity call is owned by a human engineer. Web: stabilytics.fi · Contact: ops@stabilytics.fi.

Issued by Stabilytics. Human-authored by a Stabilytics engineer. Every Critical and High finding independently peer-reviewed by a second engineer before transmission. Reports are issued under the Stabilytics name; reviewer identities are an internal coordination matter.

Questions: ops@stabilytics.fi · Web: stabilytics.fi