WHITE PAPER · VERSION 2 · OCTOBER 2026

Find, fix, **prove**.

Safe and documented changes for mobile and power networks

AIOpt AB, Gothenburg, Sweden

For network owners, grid companies and their advisers

Key message

- Two of the largest network outages of recent years started with a single, ordinary change. Neither involved AI.
- Networks are now being handed to automation and AI, which will propose far more changes than a change board can read.
- New Swedish rules ask many network owners to manage changes in a structured, traceable way and to log configuration changes.
- AIOpt runs the whole loop for network changes: it finds problems, ranks causes, recommends a fix, tests it, checks every change against the owner's rules before it runs, and keeps a signed record the owner holds.
- It has run on real 5G software in our lab and on 2.37 million rows of public research data. It has not yet run on an operator's network. The easiest first step is an offline audit of your own change history.

Contents

00 Numbers to note

01 The problem: network changes already break networks

02 Why now: software is starting to change networks by itself

03 The principle: separate who acts from who checks

04 How AIOpt works: the whole loop, with the check built in

05 Evidence so far: what we have measured, and what we have not

06 Where you are, and how to start

.. Sources

00 Numbers to note

The facts this paper rests on, each with its source

92M

calls blocked when one change took down the AT&T network, February 2024

FCC report DOC-404150A1

25,000+

failed calls to the emergency number 911 in the same outage

FCC report DOC-404150A1

12 h

about how long the AT&T network was down

FCC report DOC-404150A1

"Low"

risk rating that let a fatal Rogers change skip extra approvals, July 2022

CRTC independent review

21%

of operator respondents run at autonomy level 3 or higher today

TM Forum 2025, 141 respondents

85%

aim for level 4 by 2030, where the network changes itself

TM Forum 2025, 141 respondents

2.37M

rows of public network data read by AIOpt, none lost

AIOpt test, Sep 2026, ColO-RAN data

19/19

offline checks passed by the signed evidence pack

AIOpt test, Sep 2026, open verifier

01 The problem

Network changes already break networks

On 22 February 2024, a routine change to the AT&T network in the United States took service down for about 12 hours. 92 million calls were blocked, and more than 25,000 calls to the emergency number failed. The US regulator found that the change had been pushed without the peer review that the company's own procedures required.

In July 2022, a change in the core network of Rogers in Canada cut service for most of a day. The regulator's independent review found that the company's risk algorithm had lowered the rating of the change as earlier phases went smoothly, so extra scrutiny and approvals were skipped.

Both cases have the same shape. A change was proposed, the check that should have stopped it was skipped or weakened, and nobody could see that before customers did. Neither case involved AI. Industry writers have a name for what follows: when changes keep causing outages, operators slow down and stop changing things, even when a change would help.

02 Why now

Software is starting to change networks by itself

In TM Forum's 2025 survey of autonomous networks, 21% of operator respondents said their networks run at autonomy level 3 or higher today, 69% targeted that level for 2026, and 85% aimed for level 4 by 2030. At level 4, the network plans and acts with little human review.

A change board can read one change at a time. Automation and AI agents will propose many more, at machine speed. The question is no longer only whether a change is good, but who checks it, and whether the network owner can show afterwards what was decided and why.

New duties for network owners

Since 15 January 2026 the Swedish Cybersecurity Act (2025:1506) implements the EU NIS2 directive. For energy, transport and other sectors it covers, the regulation MCFFS 2026:11 from the Swedish Civil Defence Agency applies from 1 October 2026. Its section 30 asks for change management in the production environment "på ett strukturerat och spårbart sätt", in a structured and traceable way, and its section 21 asks for security logging that includes changes to the configuration of sector-critical systems. Telecom operators follow the Cybersecurity Act directly, with detailed rules from the telecom regulator still to come.

Regulation does not force anyone to buy a product like ours. It does make the questions concrete: which changes were approved, by whom, against which rules, and where is the record.

03 The principle

Separate who acts from who checks

Safety-critical industries learned long ago to separate the party that does the work from the party that checks it. Ship classification, aircraft maintenance release and financial audit all follow this rule. Network automation is good at proposing and making changes. What it usually lacks is a check that sits outside the system that proposed the change, and a record that the network owner keeps.

> The one who proposes a change **should not be the one** who checks it, and the owner of the network should hold the record.

This is a statement about roles, not about the quality of anyone's software. Vendors build good guardrails into their own tools. An owner running several vendors' automation, and its own staff, still needs one consistent check and one record across all of them.

04 How AIOpt works

The whole loop, with the check built in

AIOpt is not only a gate. It runs the full loop from network data to a safe change, and every step writes to the same signed record.

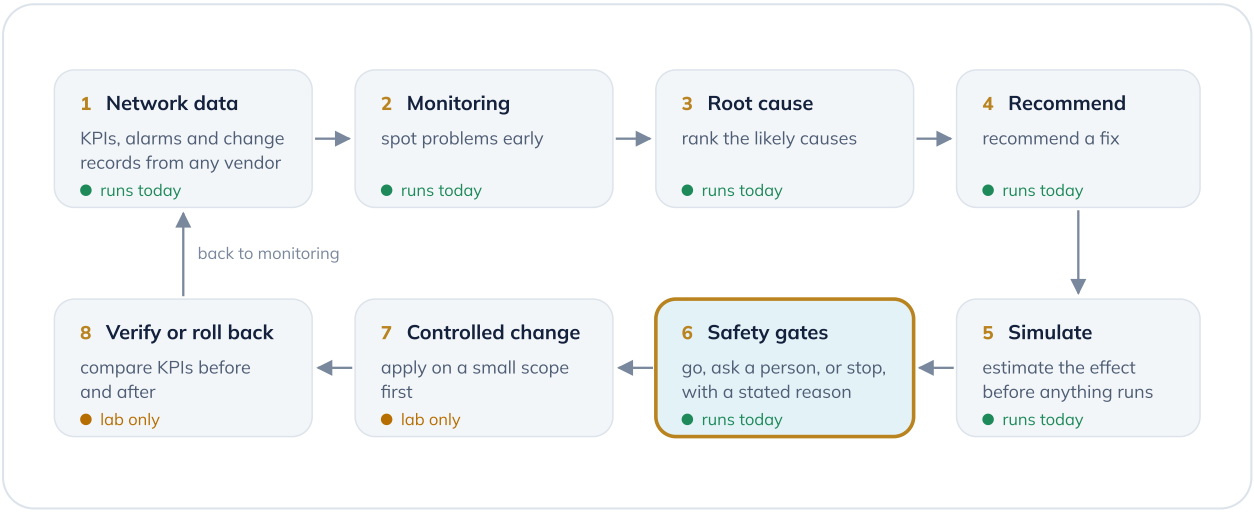


Figure 1. The loop. Every step writes to the evidence record. Steps 1 to 6 run today in our demonstrator; steps 7 and 8 have run only in our lab.
Source: AIOpt demonstrator and lab test, July 2026.

The loop matters for two reasons. A network owner gets value from the first steps, finding and explaining problems, before any change is made. And the gate in step 6 gets real proposals to judge, including AIOpt's own. AIOpt never approves its own recommendations: they face the same gate as any vendor's automation or any engineer's change.

Where it runs

AIOpt is installed inside the owner's own network and starts read-only. In the first phase it reads exported data and signs verdicts; it does not touch the network. The owner sets the rules, and the owner keeps the record.

One change, step by step

The table follows one energy-saving change through the loop. It comes from our demonstrator, on example inputs.

STEP	WHAT HAPPENS TO THIS CHANGE	WRITTEN TO THE RECORD
1 Network data	Traffic and alarm data for a cell arrive from the network.	data snapshot
2 Monitoring	Night-time traffic on the cell is low.	observation
3 Root cause	No fault is found. The cell is a candidate for saving energy.	ranked findings
4 Recommend	Put the cell to sleep for the night.	proposal and proposer
5 Simulate	Estimate whether neighbouring cells can carry the traffic.	estimate
6 Safety gates	On a normal night: go. On the night of a concert nearby: stop, with the reason that an event is planned in the area.	verdict and reason, signed
7 Controlled change	Put one cell to sleep first. `lab only`	change
8 Verify or roll back	Compare KPIs before and after, and wake the cell if they get worse. `lab only`	result, signed

The same pattern, one change allowed on a normal day and refused during a busy event, was seen on real 5G software in our lab in July 2026. Source: AIOpt demonstrator and lab test.

Step 6: the safety gates

Seven deterministic gates give one of three answers: go, ask a person, or stop with a stated reason. The network owner tunes them to its own network. They are rules, not an AI model, so the AI in earlier steps can be wrong and the check still holds. Anything unknown is refused rather than allowed.

Two of the gates come straight from the outages in chapter 1. One stops a change when a required review was skipped or a risk rating was lowered. The other refuses a change when the system that proposed it is also the one trying to approve it.

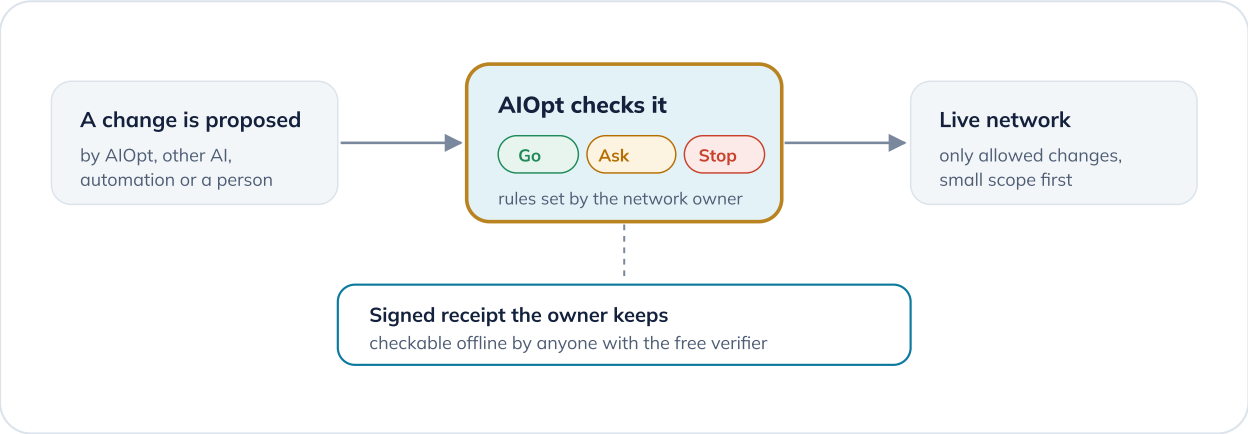


Figure 2. One decision. Refusals are recorded as carefully as approvals, because a refusal with a reason is evidence too.
Source: AIOpt product design; verifier at github.com/aiopt-se/aiopt-verify.

The record: evidence you can check without us

Every decision, approved or refused, goes into an evidence pack that the network owner keeps. Each record is signed, and the owner can countersign with its own key, so no single party can produce a valid record alone. The pack is timestamped on a public blockchain, so anyone it is shared with can check that it existed by a given date. When we tried four ways of altering a signed record, including deleting the last one, all four were detected.

The verifier that checks a pack is free and open source, shares no code with the system that writes the records, and runs offline on a laptop: github.com/aiopt-se/aiopt-verify.

05 Evidence so far

What we have measured, and what we have not

We report results as measured, with their limits. Nothing below is a customer result.

TEST 1 · JULY 2026

Our lab, on real 5G software

An open-source 5G base station (OCUDU) and core network (Open5GS) running in our lab.

- Live data arrived with no gaps: 120 measurements in 60 seconds.
- The gate allowed a change in normal conditions and refused the same change during a busy event.
- No false alarms on a healthy cell. The run first found 40, caused by a missing value filled with zero, which we fixed.

Did not show: a real operator network. One cell, no radio, no phones.

TEST 2 · SEPTEMBER 2026

Public data we did not create

The ColO-RAN research dataset, recorded on the Colosseum network emulator at Northeastern University.

- All 2,372,137 rows from 210 cell runs read. None lost.
- 168 configuration changes built from the published allocations. All were refused, each with a stated reason.
- A signed evidence pack that passes all 19 offline checks of the verifier.

Did not show: diagnosis accuracy, network improvement, or how often a harmless change is refused.

Rules have to be set for each network

The public-data run also showed why the rules belong to the network owner. A threshold that suits one network can be wrong for another.

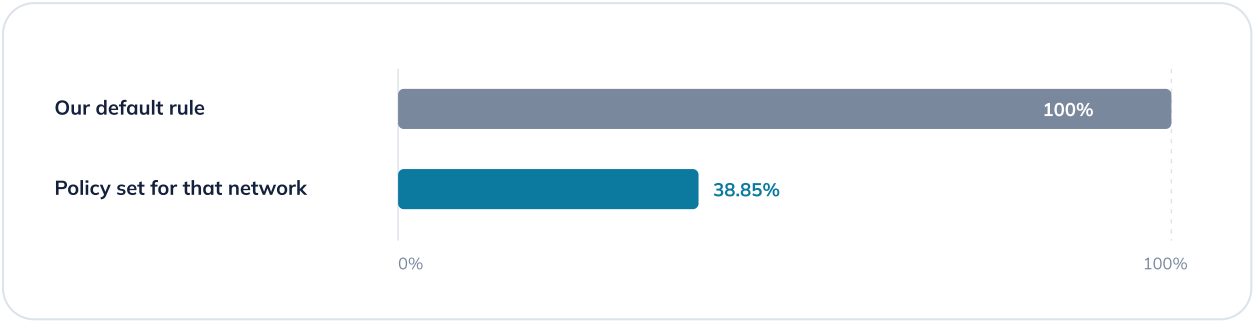


Figure 3. Rows flagged on the public dataset. Our own default threshold was wrong for that network. Rules have to be set per network, which is why the owner, not AIOpt, holds them. Source: AIOpt public-data run, September 2026, on the ColO-RAN dataset (Polese et al., 2022).

An offline replay of a million invented change records took about three minutes on a laptop. A real change history has not yet been replayed.

What we do not claim

- AIOpt has not run on an operator's or grid company's live network.
- We have no accuracy figure for the diagnosis steps; that needs real operator data.
- No outside party has yet rerun our public-data result, and no external security audit has been done.
- Controlled changes and rollback (steps 7 and 8) have run only in our lab. Automatic changes on a live network are not offered, on purpose.

06 Where you are, and how to start

Find your step on the ladder, then start read-only

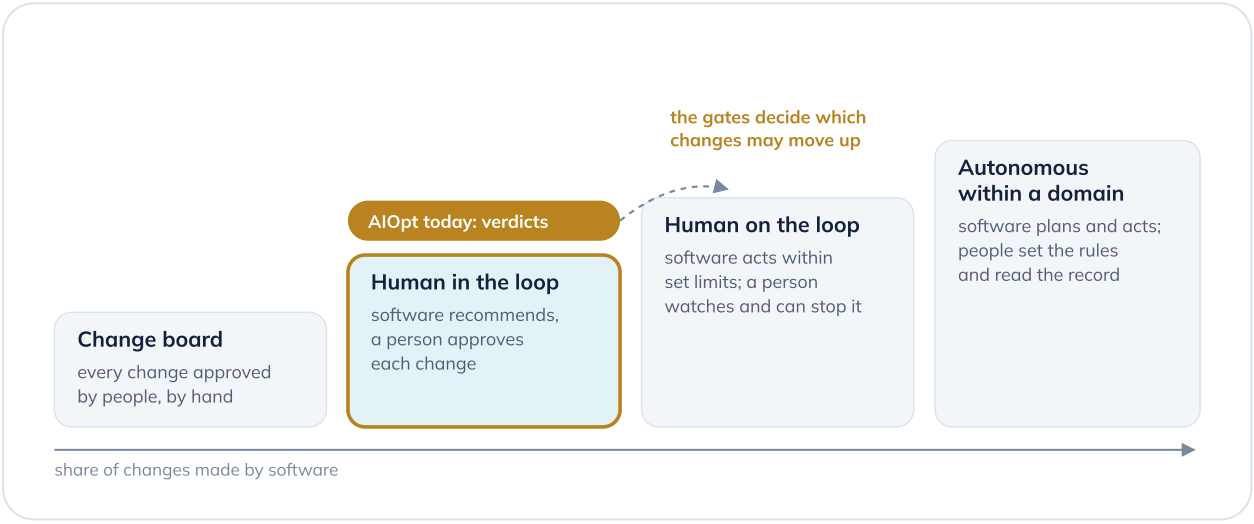


Figure 4. The autonomy ladder. AIOpt works today at the second step, signing verdicts in read-only mode. Its gates are what let an owner move individual changes up a step: changes that pass may run with a person on the loop, and the rest stay with a person.
Source: ladder wording after Appledore Research (2026); TM Forum describes the same climb as autonomy levels 0 to 5.

Five questions to place yourself

- ? How many configuration changes were made in your network last month, and by whom or by what?
- ? For each one, can you show who approved it, and against which rule?
- ? Which changes skipped a review, and would you know if one did?
- ? If an automated tool changed a setting tonight, what would stop it during a major event?
- ? Could an outsider check your change records without having to trust your tools?

First steps, read-only

If the answers are hard to give, the first steps below are built for you. None of them needs an integration, and all of them work on data you already have.

1

Discovery

`2 to 3 weeks · read-only`

Map how changes are proposed, reviewed and logged today, and replay a sample of past changes through the gates.

Done when: you have a map of your change process and a replayed sample you have agreed with.

2

Offline evidence audit

`about 4 weeks · read-only`

Export a year of change records. We replay them through the gates and report which changes would have been refused or escalated, and why, with a signed evidence pack you keep.

Done when: every exported change has a verdict and a reason, you have marked each refusal as fair or not, and you can verify the pack yourself.

For owners under MCFFS 2026:11, the report and pack support the change management of section 30 and the logging of section 21. They do not by themselves make you compliant.

3

Shadow pilot

`about 10 weeks · read-only`

AIOpt judges live changes as they are proposed and signs its verdicts, but never acts. You compare its answers with your change board's.

Done when: the success measures agreed at the start are met, for example how often AIOpt agrees with your change board and how many harmless changes it would have held back, with no effect on the network.

4

Licence

`per network domain, sized by the network`

Only after the earlier steps have shown value on your own data.

Sources

Every number in this paper traces to one of these

1. FCC, Public Safety and Homeland Security Bureau. Report on the February 22, 2024 AT&T Mobility network outage. Document DOC-404150A1. docs.fcc.gov/public/attachments/DOC-404150A1.pdf
2. CRTC. Staff letter to Rogers Communications on the independent assessment of the July 2022 outage, 22 December 2023. crtc.gc.ca/eng/archive/2023/lt231222c.htm
3. Summary of the CRTC's independent review of the Rogers outage, July 2024. mobilesyrup.com/2024/07/05/july-2022-rogers-outage-report-crtc
4. TM Forum. A regional guide to autonomous networks progress, 2025. Base: 141 respondents from operators. info.tmforum.org
5. Myndigheten för civilt försvar. MCFFS 2026:11, in force 1 October 2026, sections 21 and 30. mcf.se
6. Cybersäkerhetslag (2025:1506), in force 15 January 2026.
7. Google Cloud, Vodafone and TM Forum. Self-optimizing autonomous networks: an implementation guide, June 2026 (the slowdown that follows change-caused outages). services.google.com
8. Appledore Research for Amdocs. Autonomous network operations research note, April 2026 (the human-in-the-loop to autonomous ladder). amdocs.com
9. Polese et al. ColO-RAN: Developing machine learning-based xApps for open RAN closed-loop control on programmable experimental platforms. IEEE Transactions on Mobile Computing, 2022. Dataset: github.com/wineslab/colosseum-oran-coloran-dataset
10. AIOpt verifier, open source (MIT). github.com/aiopt-se/aiopt-verify

About AIOpt

AIOpt AB was founded in Gothenburg, Sweden, in 2024. It builds software that finds problems in mobile and power networks, recommends fixes, and checks every change before it runs, with a signed record the network owner keeps.

Contact

Write to `support@aiopt.se` or visit aiopt.se. To try the verifier yourself, start at the GitHub link above.

Version 2, 22 October 2026