DC False Alerts: Could TCAS Be Vulnerable to Cyber Attack?

Chris Shieff
10 March, 2025

On March 1, several aircraft reported erroneous TCAS TA and RA alerts while on approach to Runway 19 at **KDCA/Washington.** All aircraft correctly followed avoidance procedures, and **no loss of separation** occurred. Six of the incidents occurred within eleven minutes of each other.

⬆ *shared with permission, courtesy of **VASAviation.***

What has followed is speculation – who, or what, was responsible? It is an answer the FAA is actively seeking.

TCAS interference is rare but can occur. There are several plausible explanations including ground clutter and reflections, software issues and unintentional radio interference.

However, it would be hard to deny that these alerts came at a **sensitive time** both for operations at the airport following the mid-air collision over the Potomac River, and across a broader tapestry of concern for aviation safety across the US NAS given recent events.

Which begs an important question – **can TCAS actually be tampered with?** Is it possible these events were an act of criminal mischief or other mis-intent? While remote, a little-known alert issued just weeks ago by **CISA** (the part of Homeland Security responsible for US cyber and infrastructure security) suggests it is *indeed* possible.

Published on January 21, CISA discussed **two flaws in TCAS design** that leave the system vulnerable to **malicious cyber-attacks** – one of which they deem a high, almost critical vulnerability.

In event that such an attack occurs, criminal interference could generate fake targets on an aircraft's TCAS display and even disable resolution advisories.

The problem is that bulletin is quite technical. So here is a break-down of what it says in plain, simple language.

The Bulletin

There were essentially two risks identified for TCAS II Versions 7.1 or older.

1. Fake Position Signals

It is theoretically possible to broadcast a spoofed aircraft location to another target.

This could be achieved using specialised radio equipment where potential attackers could send fake signals to aircraft, causing the appearance of **non-existent targets** on TCAS displays, along with the associated warnings.

In other words, crews would effectively be chasing shadows.

As TCAS II systems rely on transponders that may not be able to adequately validate the data received, they remain vulnerable to unauthorised signals. The bulletin describes this risk as a reliance on ‘*untrusted inputs’.*

Read the report and you’ll see something called a ‘**CVSS score.’**

CVSS stands for **Common Vulnerability Scoring System**, and it is basically a danger rating for flaws in computer security. It is a measure of how serious a vulnerability is. Factors include the method of attack, the access required and the potential impact.

It is represented on a scale of 0 (non-existent) to 10 (critical).

The issue of fake position signals has been given a CVSS score of 6.1.

Perhaps more concerning is that the report advises there is no way to actively mitigate this threat with existing TCAS technology. The equipment required is accessible to the public. Therefore this threat is the most likely suspect of any erroneous TCAS interference occurring today.

2. No TCAS RA

This affects some older TCAS II systems using transponders with outdated technical standards.

It is theoretically possible for an attacker to impersonate a ground station and send a special request that lowers a system’s sensitivity settings. A TCAS sensitivity level command does exist, envisaged to reduce nuisance alerts at some airports.

This could be used to maliciously adjust sensitivities to the lowest setting and even **disable a resolution advisory** completely.

The threat has a concerning CVSS score of 8.1 – highly vulnerable to exploitation, but would require a high level of expertise and technology to carry out.

Fortunately, in this case there is a way to mitigate the problem – by switching to ACAS X, or upgrading your associated transponder to more recent technical standards.

There is **no indication** that this has vulnerability has ever been exploited.

While unlikely, the CISA bulletin proves that TCAS could be vulnerable to malicious interference.

So, could the aircraft at KDCA have been hacked?

It’s unlikely, but CISA’s report indicates it’s possible. And a new expert analysis of events at KDCA by **Aireon** seems to agree. In their published report they found that *‘it is possible the intruder was airborne or related to a ground-based transmitter used for testing or spoofing.’*

Why does this matter?

The industry must remain responsive to security threats that are becoming increasingly sophisticated and designed to exploit vulnerabilities in safety critical systems.

The recent industry-wide interest in GPS interference spanning from the inconvenient, to major degradations including the loss of EGPWS protection, ADS-B tracking and navigational accuracy is a startling testament to this fact. This is all possible because of **existing system design.**

Since the events of September 11, passenger screening and security protocols have undergone a revolution, and it’s now much harder for bad actors to carry out conventional attacks. But there are still risks associated with malicious attacks that could potentially be achieved **remotely** – and cyber-interference seems an obvious choice.

(No More) Danger in Denver

Chris Shieff
10 March, 2025

Back in 2022, the FAA issued a Safety Alert (SAFO) for KDEN/Denver, after a **high number of TCAS RA events** were recorded between aircraft landing on the parallel runways (16L/16R).

This was compounded by a number of factors:

- **High elevation**
- **Reduced separation**
- **Controller workload**
- **Possible complacency caused by regular nuisance TAs.**

It was a moody brew leading to the FAA becoming concerned about potential for a **midair collision.** If you're like to know more, here's an article we wrote at the time.

The good news is that last month, **new approaches** were introduced to alleviate the risk. Here's an update on what has changed.

Offset Approaches

On November 30, Runway 16R received two new approaches **(offset by 3 degrees)** – the RNAV (Y) and RNP (Z).

It was previously determined that 3-degrees would be enough to mitigate nuisance TCAS activations and allow operators to continue using full TA/RA mode throughout their approach and landing.

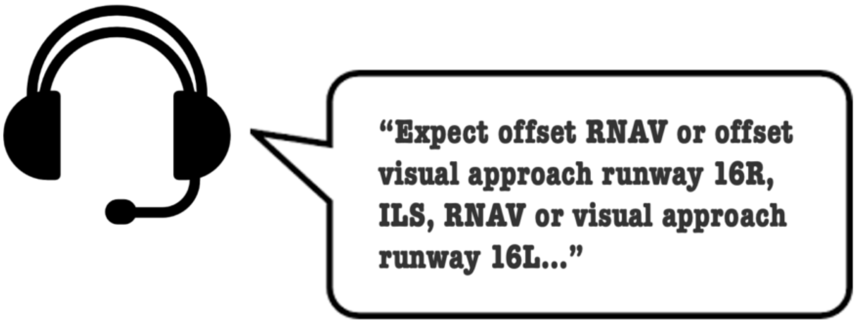
Along with these offset approaches, the FAA has published **new procedures** for their use found in this Information Note for Operators.

The procedures will be in use anytime Runways 16L and R are operating simultaneously, and **visual**

approaches are in use on at least one of the runways.

New Procedures

Listen out for the following phrase on the ATIS:


"Expect offset RNAV or offset visual approach runway 16R, ILS, RNAV or visual approach runway 16L..."

If you're landing on 16R, there are effectively now two scenarios:

Instrument Approach – Follow the RNAV (Y) or RNP (Z) charted procedure. Easy.

or

Visual Approach – Here's where things get a little more complicated. Even though the FAA regs say that an aircraft on a visual approach does not need to follow a specific track or vertical profile, in the case of KDEN, the FAA **strongly suggests** you do.

Aside from assuring you stay inside Class B airspace, it will also mitigate nuisance TCAS RA's that can lead to unstable approaches, go-arounds and level busts.

In their Info Note the FAA goes even further and says **don't fly a straight-in approach to 16R** (including via the existing ILS) unless **specifically cleared** to do so.

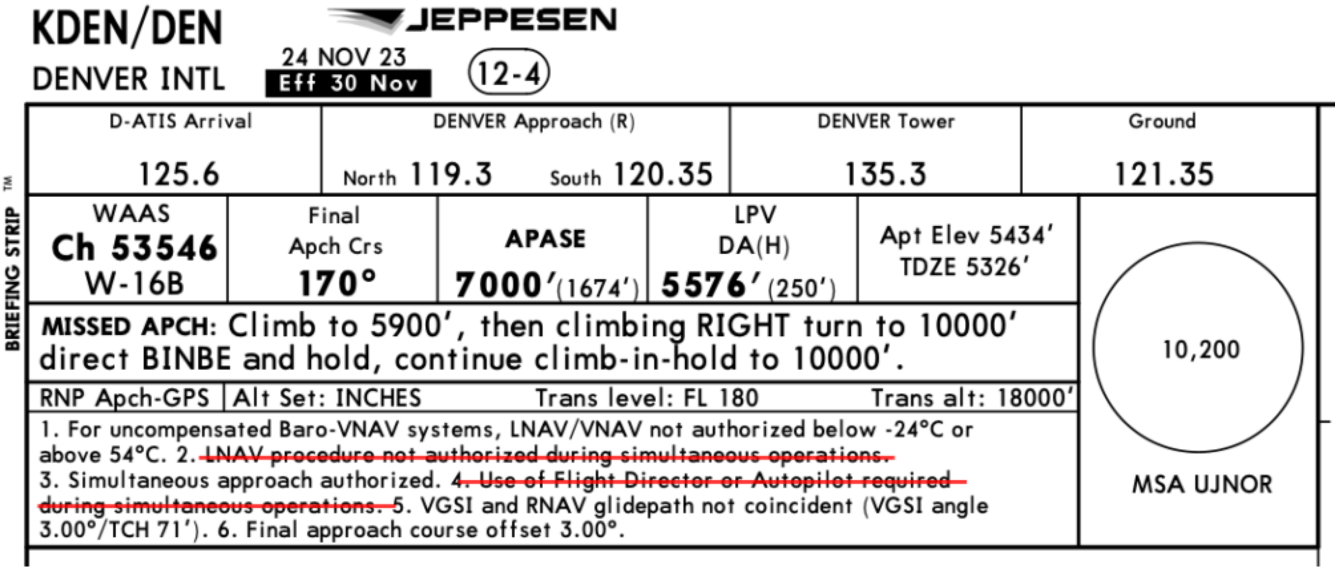
So when can we line up with the runway?

Whether you are on an instrument approach, or a visual, the FAA says don't break off the offset until you can see the runway and have **crossed the FAF.**

Look out for these chart notes...

Because the above procedure will only be used when conditions permit a visual approach on at least one of the two parallel runways, technically the whole deal doesn't fall within the realm of *'simultaneous IFR operations.'*

So, you can disregard the following two chart notes:



KDEN/DEN
DENVER INTL

JEPPESEN
24 NOV 23
Eff 30 Nov
12-4

BRIEFING STRIP ™

D-ATIS Arrival	DENVER Approach (R)	DENVER Tower	Ground
125.6	North 119.3 South 120.35	135.3	121.35

WAAS	Final Apch Crs	APASE	LPV DA(H)	Apt Elev 5434'
Ch 53546 W-16B	170°	7000'(1674')	5576'(250')	TDZE 5326'

MISSED APCH: Climb to 5900', then climbing RIGHT turn to 10000' direct BINBE and hold, continue climb-in-hold to 10000'.

RNP Apch-GPS | Alt Set: INCHES | Trans level: FL 180 | Trans alt: 18000'

1. For uncompensated Baro-VNAV systems, LNAV/VNAV not authorized below -24°C or above 54°C. 2. ~~LNAV procedure not authorized during simultaneous operations.~~ 3. Simultaneous approach authorized. 4. ~~Use of Flight Director or Autopilot required during simultaneous operations.~~ 5. VGSI and RNAV glidepath not coincident (VGSI angle 3.00°/TCH 71'). 6. Final approach course offset 3.00°.

10,200
MSA UJNOR

…although the last one is still recommended by the FAA.

Still have questions?

You can get in touch with the folk at the Flight Technologies and Procedures Division at 9-AWA-AVS-AFS-400-Flight-Technologies-Procedures@faa.gov (yes, that's the real address) or on the phone via (202) 267- 8790.

Or talk to us! team@ops.group. We'd love to hear from you.

Is TCAS always required on the North Atlantic?

Andy Spencer
10 March, 2025

Oh, TCAS, you sly little gadget! The Traffic Collision Avoidance System is the knight in shining armour for preventing mid-air collisions. **You would think that TCAS would be an absolute must-have in the NAT airspace**, where the skies are busier than a beehive. But wait for it… surprise, surprise, the answer is a RESOUNDING (but actually slightly complicated) **NO!**

How can this be?

Although most aircraft are still required to have TCAS onboard, a little something called **MEL dispensation** comes to the rescue.

Minimum Equipment List (MEL) is like that cool aunt who lets you get away with stuff. **It allows us to operate with TCAS inoperative, within certain limits.** For some aircraft, it's a two-day pass, while others enjoy ten whole days of TCAS-less adventures (as long as they're departing from a place where fixing it isn't possible).

But what about ATC? Don't they require us to have functioning TCAS?

We reached out to **Shanwick ATC** for a comment, and they had something surprising to say:

- *Shanwick supervisor guidelines state that there are no operational reasons for ATC to refuse a request to operate in Shanwick without functioning TCAS.*
- *There are some caveats: level or route restrictions may be imposed to avoid densely populated airspace, however this is unlikely within Shanwick airspace. ATC here would not automatically exclude the flight from the NAT Tracks. Operators should file and request their optimal routing and ATC will endeavour to approve as requested.*
- *Where TCAS fails during flight: Shanwick ATC will coordinate with the next unit but advise that the operator should be coordinating with other ANSPs, particularly those without a NAT boundary (for example any Eastbound flight that suffers TCAS failure in Gander FIR – Gander would coordinate with Shanwick and Shanwick would coordinate with Shannon).*

A discussion with **Gander ATC** on the other side of the pond resulted in much the same information:

- *There is no rule prohibiting an aircraft operating under TCAS MEL relief from operating anywhere in the NAT HLA or on the NAT Tracks.*

It all boils down to **airspace design and risk mitigation.** When intelligent folks design these controlled airspace areas, they put the responsibility of traffic separation on ATC. So, whether we have TCAS or not, it keeps their game plan the same. Our fancy onboard collision avoidance measures, whether TCAS or a creative SLOP manoeuvre, are like sprinkles on the icing of the airspace cake.

A word of caution

MEL isn't there to make us feel invincible. **It's not a license to fly with broken stuff just because we can.** It's more like a get-out-of-jail-free card to prevent us from being stranded without a paddle.

And also, before making grand plans for TCAS-free adventures, remember that **our departure and destination airports may have something to say about it.** The busier places like London or New York might only be keen on welcoming an aircraft with TCAS.

So, what are our options? We might need to make a detour to a quieter second or third-tier airport, which might not be as glamorous as our passengers desire. We'll have to calculate the impact on remaining time and fuel and consider getting our aircraft to a maintenance base before the MEL expires.

Gimme the bite-sized version

- En-route ATC centres don't have any operational reasons to refuse entry into the NAT. **If it breaks before the flight, you must let all of them know.** If it breaks in flight, they will help you.
- You may not get your planned level or track – **you will need more fuel** as a contingency.
- Be mindful that the **MEL doesn't intend us to fly with broken equipment simply because we can**… it's a tool for us to get aircraft to equipped maintenance centres
- **Your departure or destination airports may not accept you without TCAS.** Consider where you would go and how that would impact the remaining time of deferred defects.

Danger in Denver: Collision Risk

Chris Shieff
10 March, 2025

On August 3, the FAA put out a new Safety Alert (SAFO) for KDEN/Denver. Here it is if you want a read.

The issue is the high number of TCAS alerts being recorded when aircraft are shooting parallel approaches to Runways 16L/16R.

It turns out that TCAS, high elevation, and reduced separation aren't a great mix, and the FAA are worried there are chances of a collision.

Here's a breakdown of the situation.

Elbow to Elbow.

Since 2004, KDEN has been operating two parallel runways (16L and R). The two runways sit literally elbow to elbow, with only 2600' (709m) between them. For simultaneous close parallel approaches, 3600′ separation between runway centrelines is generally required. In Denver, typically two separate controllers are feeding traffic onto the approach cones for each runway, which means **coordination can be a challenge.**

From early on it became apparent that **nuisance TCAS alerts were a problem.** The FAA sought to fix the issue, and so in June 2019 Denver TRACON started separating aircraft vertically by 1000' in case someone busted through a localizer.

Trouble is, this didn't fix the issue. Instead, now the **majority of TCAS events are happening when aircraft are established on the final approach course.** The big threat here is the number of folk selecting TA only (a good 20%), and there is now a healthy dose of desensitisation thrown into the mix from so many nuisances warnings in the past.

Then there's the elevation.

Fun fact: TCAS becomes more sensitive with altitude. Or in other words, the trigger thresholds for both TAs and RAs increase the higher you get.

Enter Denver – the '*Mile High City*' – called that because it sits exactly a mile above sea level. **That's around a 5,300' elevation.**

The next iteration of TCAS, (the romantically named ACAS XO), promises better tolerances for these conditions but it's not here yet, so right now users of **TCAS 7.1 get all the warnings when all the warnings are not necessary.**

What the FAA are concerned about.

Operate into Denver, and the threat of simultaneous parallel approaches isn't new, but awareness of the threats needs to be improved. The basic idea is folk should:

- Have an awareness of how the **close in approach setup** might increase the threat
- Brief how operating in **TA only mode** adds to this
- Know exactly where to be and what's around by **listening out on the radio** and monitoring TCAS carefully
- Think about to remember to **re-select TA/RA mode** in the event of a missed approach
- Be aware of how **nuisance TCAS** cautions and warnings may **desensitize** crew.

In fact, this could be useful guidance anywhere where there are similar operational and environmental conditions which might increase the risk of collision.

TCAS Trouble: Why We’re Getting It Wrong

Chris Shieff
10 March, 2025

Earlier this year Eurocontrol published a report on TCAS Resolution Advisories, and the results weren’t pretty…

Over a 12-month period, over the heart of Europe, only 38% of RAs were flown correctly and **34% of aircraft even manoeuvred in the wrong direction.**

In other words, **nearly half of crew for one reason or another didn’t follow the RA** – a last-resort safety net proven to save lives. So concerned are Eurocontrol, they rank the issue as its **second highest air traffic threat** – it’s a big deal.

Here’s the issue in a nutshell

ICAO say that no matter what, unless the safety of your aircraft is compromised by something more dangerous (think terrain or stall etc.) if you get an RA, **you have to follow it**.

TCAS, ACAS or whatever you want to call it has been around for a long time. Development started back in the 50s, and it has been mandated in the US for larger aircraft since the 80s. It has become incredibly reliable.

So, if it’s that black and white, the question remains, **why does this keep on happening?** Turns out there are a bunch of reasons, and so it is worth taking a look at exactly what is going wrong up there.

The Elephant in the Room

We may as well address it first – when crew choose to second guess an RA. The good news is that this isn’t happening very often. Most of the time there are other factors at play. But while we’re here, a little note on TAs and RAs.

Traffic Advisories (TA) **prevent**. You haven't lost separation yet, but you might. They're a warning for us to go heads up and do something about it – make visual contact, talk to ATC, level off, you name it. This is the time for us to go to work and make decisions.

Resolution Advisories (RA) **mitigate**. There is no more time to prevent – **that ship has sailed.** RA's typically trigger when you are within 25 seconds of a collision threat with the other aircraft. But here's the kicker – you are expected to respond to it within 5 seconds. In other words, there is not much time for us to make effective decisions. Safest course of action? You guessed it – **follow the RA.**

So, what else is going on then?

Numero Uno – The number 1 biggest reason why RAs aren't followed? Because we think **we can see the threat out the window.** Unfortunately, you can't assume that the aircraft you can see is the one who triggered the RA. We're also not very good at assessing threats visually, especially at altitude and it does not give us any info about what the other aircraft is intending to do.

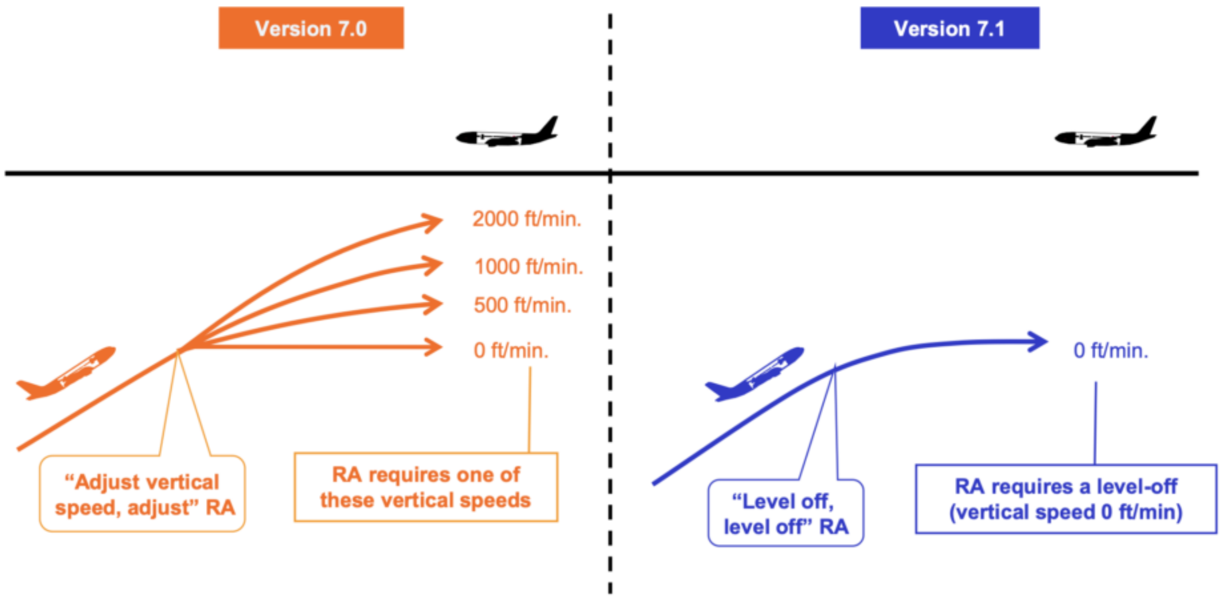
Startle Factor – Put us in a stressful situation and we react in different ways. RA's are a rare event, and they're **not always preceded with a TA.** In other words, without warning they can emerge with significant 'pucker factor'. A large number of mis-flown RAs in the EUROCONTOL report lasted for less than 8 seconds. Beware of the **'knee jerk' reaction** – our instinct is to act but surprise can get in the way of procedure.

Beware of Contradictions – It's not ATC's fault, but it's important to understand. They don't know what your TCAS is telling you to do and they will be working hard to help. The issue is when **ATC instructions contradict your RA**. In 2002, a Tupolev passenger jet collided with a 757 over Germany – one crew followed the RA and the other ATC. The industry learnt an important lesson: **always follow the RA**. Use the phrase "TCAS RA" on the radio and ATC will understand you are following one.

Performance – RA's are often not followed as the crew are **worried about performance.** This usually happens when they're heavy and high or near their service ceiling and get a climbing RA. So, what should you actually do? The official word is this: **do your best to follow it**, even if your response is weak. Even if it means maintaining your level. In most cases an RA will only result in a level change of less than 500 feet. The biggest threat by far is opposing the RA, which will put your aircraft in far more danger.

Training – That old chestnut. But the reality is it is really important to practice these things in the sim. Weird ones. Unexpected ones. Ugly ones. Ones with multiple threats. Because this is usually what we're up against in **the real world.** Also keep your finger on the pulse for changes. Some modern aircraft can now fly RA's automatically, but the sims you train in may not have had the same update.

Older Versions – watch out for them. The latest one (7.1) has a number of major safety updates including clearer instructions and 'reversals' – a fancy term for knowing when the other aircraft isn't doing what it is supposed to do. Older versions of TCAS are more likely to be misunderstood by crew. One phrase in particular is especially bad – "Adjust Vertical Speed, Adjust." In many cases crew have increased their vertical speed rather than reduce it. If you're using older versions it is important to be aware of its limitations.


Version 7.0
Version 7.1
2000 ft/min.
1000 ft/min.
500 ft/min.
0 ft/min.
"Adjust vertical speed, adjust" RA
RA requires one of these vertical speeds
0 ft/min.
"Level off, level off" RA
RA requires a level-off (vertical speed 0 ft/min)

TCAS is an awesome piece of kit that has made huge advances in preventing completely avoidable accidents. But it is only as reliable as the humans who respond to it. That's why it is so important we learn about what we we're getting wrong so it can do its job – keeping us safe up there.

Other Useful Things

- Eurocontrol's recent report on RA non-compliance
- The FAA's Guide to TCAS 7.1 (the latest version)