A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

Matt Smith[$], Martin Strohmeier[$†], Jonathan Harman, Vincent Lenders[†] and Ivan Martinovic[$]

[$]Department of Computer Science,
University of Oxford,
United Kingdom
Email: first.last@cs.ox.ac.uk
Twitter: @avsecoxford

[†]Cyber-Defence Campus,
armasuisse Science + Technology,
Switzerland
Email: first.last@armasuisse.ch
Twitter: @cydcampus

Network and Distributed Systems Symposium (NDSS) 2020

23-26th February 2020

Security Research in Aviation

Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeastern University, Boston, MA, USA

USENIX 2019

Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeaster

USENIX 2019

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

Matthias Schäfer[1], Vincent Lenders[2], and Ivan Martinovic[3]

ACNS 2013

Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeastern

USENIX 2019

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

ACNS 2013

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
Network and Security Department
EURECOM
Sophia-Antipolis, France
Email: andrei.costin@eurecom.fr, aurelien.francillon@eurecom.fr

Blackhat 2012

Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeaster

USENIX 2019

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

ACNS 2013

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
Network and Security Department

Blackhat 2012

Exploring the Vulnerabilities of Traffic Collision Avoidance Systems (TCAS) Through Software Defined Radio (SDR) Exploitation

Paul M. Berges

Masters Thesis, 2019

Security Research in Aviation

Wireless A

Harshad Sathay

Northeastern

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer, Dept. of Computer Science, ETH Zurich, Switzerland, tinils@inf.ethz.ch
Christina Pöpper, Dept. of Computer Science, ETH Zurich, Switzerland, poepperc@inf.ethz.ch
Kasper B. Rasmussen, Computer Science Dept., UCI, Irvine, CA, kbrasmus@ics.uci.edu
Srdjan Čapkun, Dept. of Computer Science, ETH Zurich, Switzerland, capkuns@inf.ethz.ch

CCS 2011

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

ACNS 2013

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
Network and Security Department

Blackhat 2012

Exploring the Vulnerabilities of Traffic Collision Avoidance Systems (TCAS) Through Software Defined Radio (SDR) Exploitation

Paul M. Berges

Masters Thesis, 2019

Security Research in Aviation

Wireless A…

Harshad Sathay…

Northeastern…

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer
Dept. of Computer Science
ETH Zurich, Switzerland
tinils@inf.ethz.ch

Christina Pöpper
Dept. of Computer Science
ETH Zurich, Switzerland
poepperc@inf.ethz.ch

Kasper B. Rasmussen
Computer Science Dept.
UCI, Irvine, CA
kbrasmus@ics.uci.edu

Srdjan Čapkun
Dept. of Computer Science
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

CCS 2011

Experimental Analysis of Attacks on Next …

Hacker + Airplanes = No Good Can Come Of This

RENDERMAN CHIEF RESEARCHER

DEF CON 20

Ghost in the Air(Traffic): On insecurity of ADS… ADS-B devic…

Andrei Costin, Aurélien Francillon
Network and Security Department

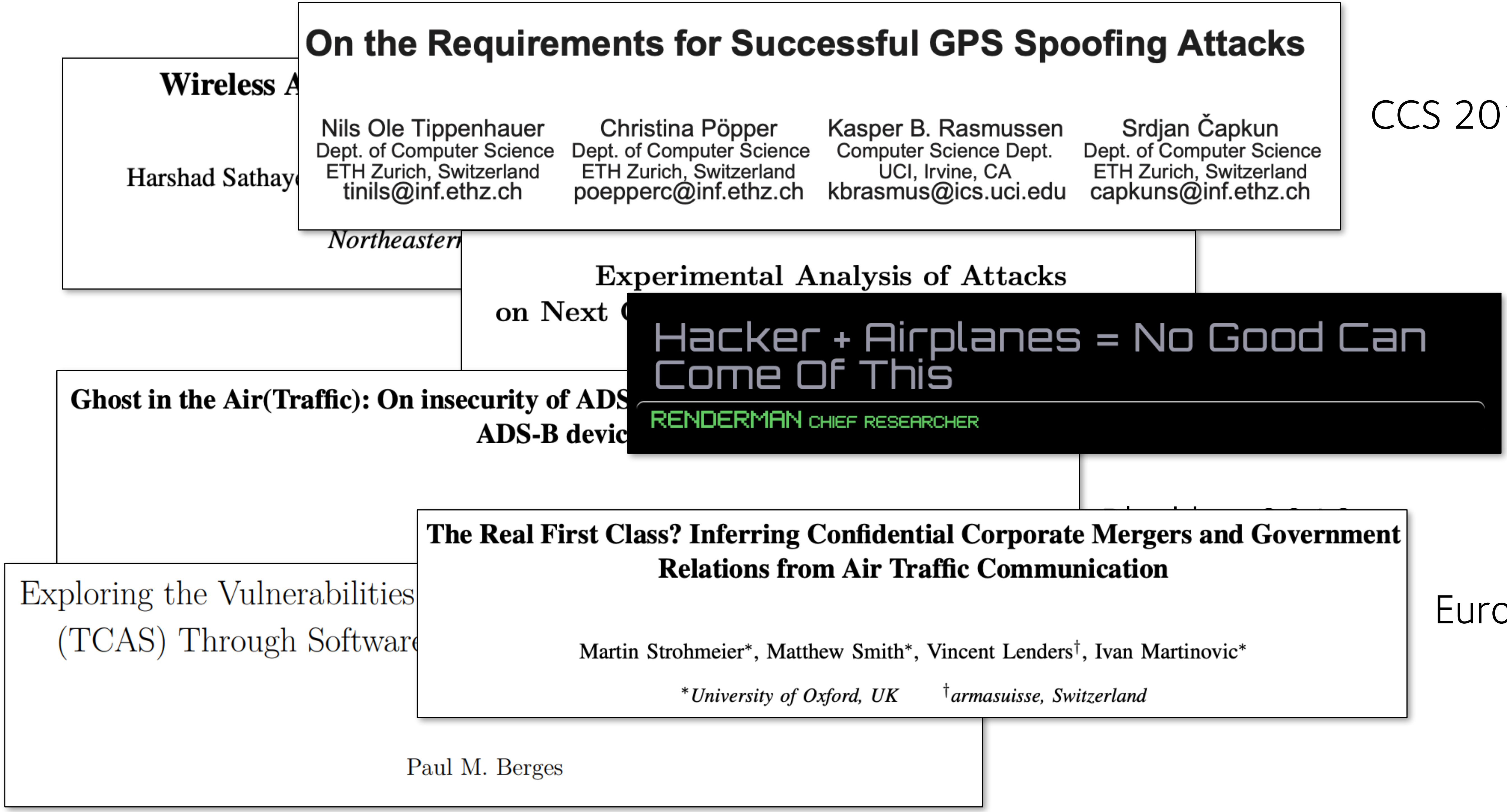
Blackhat 2012

Exploring the Vulnerabilities of Traffic Collision Avoidance Systems (TCAS) Through Software Defined Radio (SDR) Exploitation

Paul M. Berges

Masters Thesis, 2019

Security Research in Aviation


Wireless A

Harshad Sathay

Northeastern

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer, Dept. of Computer Science, ETH Zurich, Switzerland, tinils@inf.ethz.ch
Christina Pöpper, Dept. of Computer Science, ETH Zurich, Switzerland, poepperc@inf.ethz.ch
Kasper B. Rasmussen, Computer Science Dept., UCI, Irvine, CA, kbrasmus@ics.uci.edu
Srdjan Čapkun, Dept. of Computer Science, ETH Zurich, Switzerland, capkuns@inf.ethz.ch

Experimental Analysis of Attacks
on Next

Hacker + Airplanes = No Good Can Come Of This
RENDERMAN CHIEF RESEARCHER

Ghost in the Air(Traffic): On insecurity of ADS
ADS-B devic

The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication

Martin Strohmeier*, Matthew Smith*, Vincent Lenders†, Ivan Martinovic*

*University of Oxford, UK †armasuisse, Switzerland

Exploring the Vulnerabilities
(TCAS) Through Software

Paul M. Berges

CCS 2011

DEF CON 20

EuroS&P 2018

Security Research in Aviation

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer, Dept. of Computer Science, ETH Zurich, Switzerland, tinils@inf.ethz.ch
Christina Pöpper, Dept. of Computer Science, ETH Zurich, Switzerland, poepperc@inf.ethz.ch
Kasper B. Rasmussen, Computer Science Dept., UCI, Irvine, CA, kbrasmus@ics.uci.edu
Srdjan Čapkun, Dept. of Computer Science, ETH Zurich, Switzerland, capkuns@inf.ethz.ch

CCS 2011

Wireless A

Harshad Sathay

Northeaster

Experimental Analysis of Attacks
on Next G

Hacker + Airplanes = No Good Can Come Of This
RENDERMAN CHIEF RESEARCHER

DEF CON 20

Ghost in the Air(Traffic): On insecurity of ADS
ADS-B devic

The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication

Martin Strohmeier*, Matthew Smith*, Vincent Lenders†, Ivan Martinovic*

**University of Oxford, UK* †*armasuisse, Switzerland*

EuroS&P 2018

Exploring the Vulnerabilities
(TCAS) Through Software

How well do pilots handle these attacks?

Last Line of Defence

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator

Baltic Aviation Academy, Wikipedia [5]

Last Line of Defence

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator

They also form a 'last line of defence' against faults, through well-defined procedure

Baltic Aviation Academy, Wikipedia [5]

Last Line of Defence

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator

They also form a 'last line of defence' against faults, through well-defined procedure

How well does fault-handling skill translate to attack mitigation?

Baltic Aviation Academy, Wikipedia [5]

Last Line of Defence

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator

They also form a 'last line of defence' against faults, through well-defined procedure

How well does fault-handling skill translate to attack mitigation?

Can we use flight simulation to understand the impact of attacks?

Baltic Aviation Academy, Wikipedia [5]

Method

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator

Photo of simulator set up

Method

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems

Photo of simulator set up

Method

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems
- Uses XPlane 11 with a high-quality aircraft model
- Experimenter provided flying support (enabling modes/ pressing buttons on command)

Photo of simulator set up

Method

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems
- Uses XPlane 11 with a high-quality aircraft model
- Experimenter provided flying support (enabling modes/ pressing buttons on command)

Protocol

1. Familiarisation flight
2. For each attack:
    a) Simulator flight including attack
    b) Debrief interview about flight
3. Overall debrief interview

Photo of simulator set up

Method

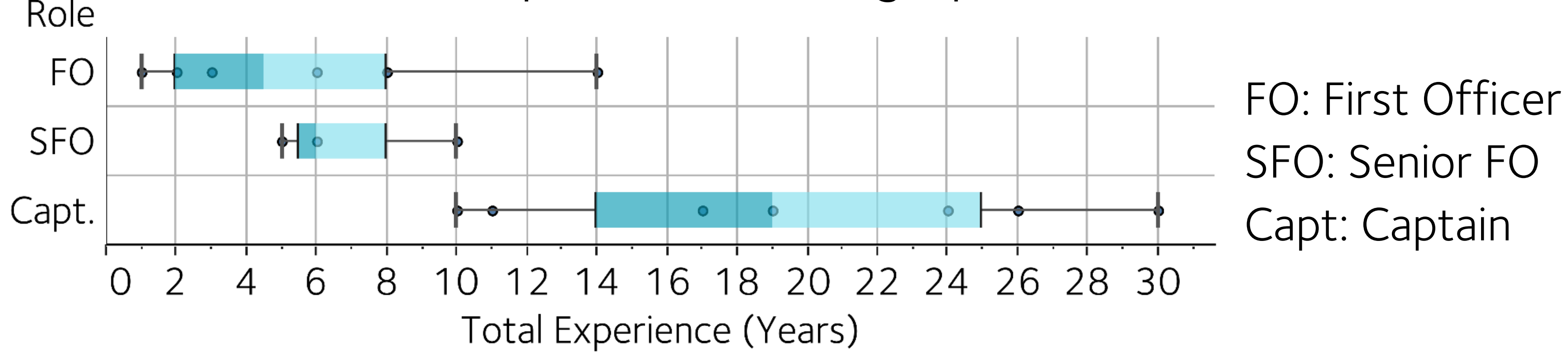
- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems
- Uses XPlane 11 with a high-quality aircraft model
- Experimenter provided flying support (enabling modes/ pressing buttons on command)

Protocol

1. Familiarisation flight
2. For each attack:
    a) Simulator flight including attack
    b) Debrief interview about flight
3. Overall debrief interview

Photo of simulator set up

Experience demographics



Attacker Model

Capabilities

Motivation	Cause delay, financial loss, reputational harm or a reduction in safety

Attacker Model

Capabilities

Motivation	Cause delay, financial loss, reputational harm or a reduction in safety
Means	• Trigger go-arounds • Force unexpected maneuvers • Push crew to switch systems off

Attacker Model

Capabilities

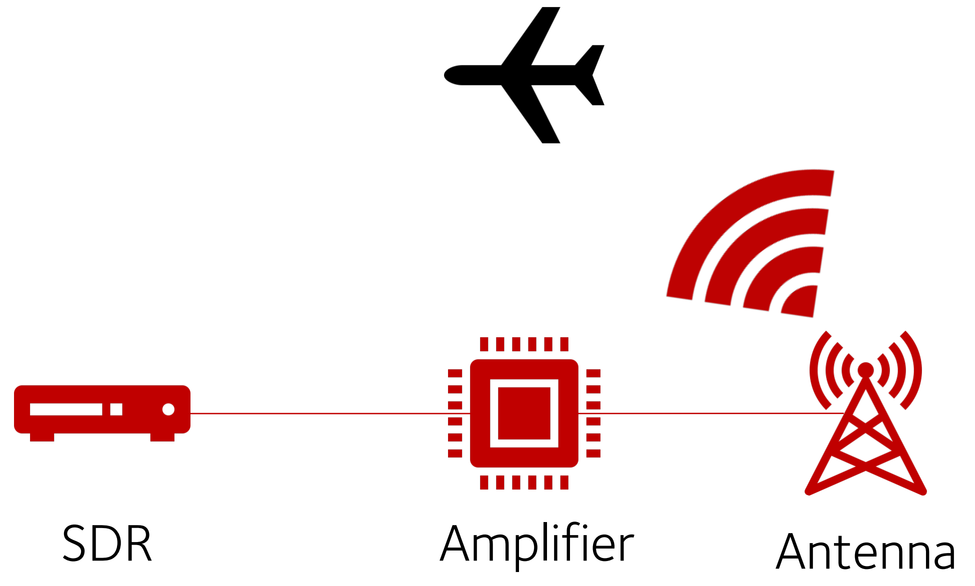
Motivation	Cause delay, financial loss, reputational harm or a reduction in safety
Means	• Trigger go-arounds • Force unexpected maneuvers • Push crew to switch systems off
Ability	• Understanding of avionics standards/ systems • Ability to create radio software for attacks • Deploy in a single or multiple locations

Attacker Model

Capabilities

Motivation	Cause delay, financial loss, reputational harm or a reduction in safety
Means	• Trigger go-arounds • Force unexpected maneuvers • Push crew to switch systems off
Ability	• Understanding of avionics standards/ systems • Ability to create radio software for attacks • Deploy in a single or multiple locations

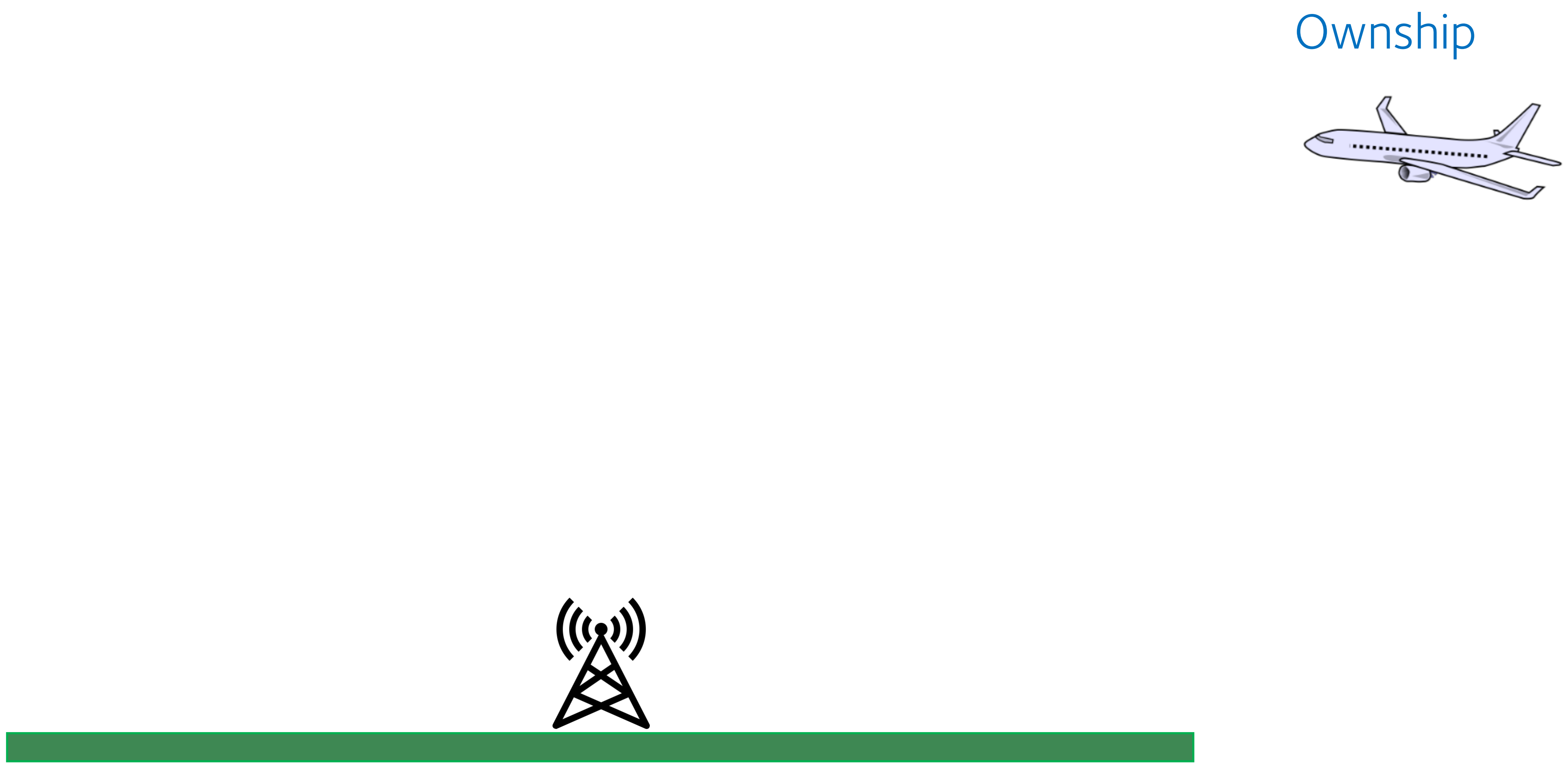
Equipment



- Scientific-grade Software Defined Radio (SDR) e.g. Ettus USRP
- High-gain amplifier
- Directional antenna

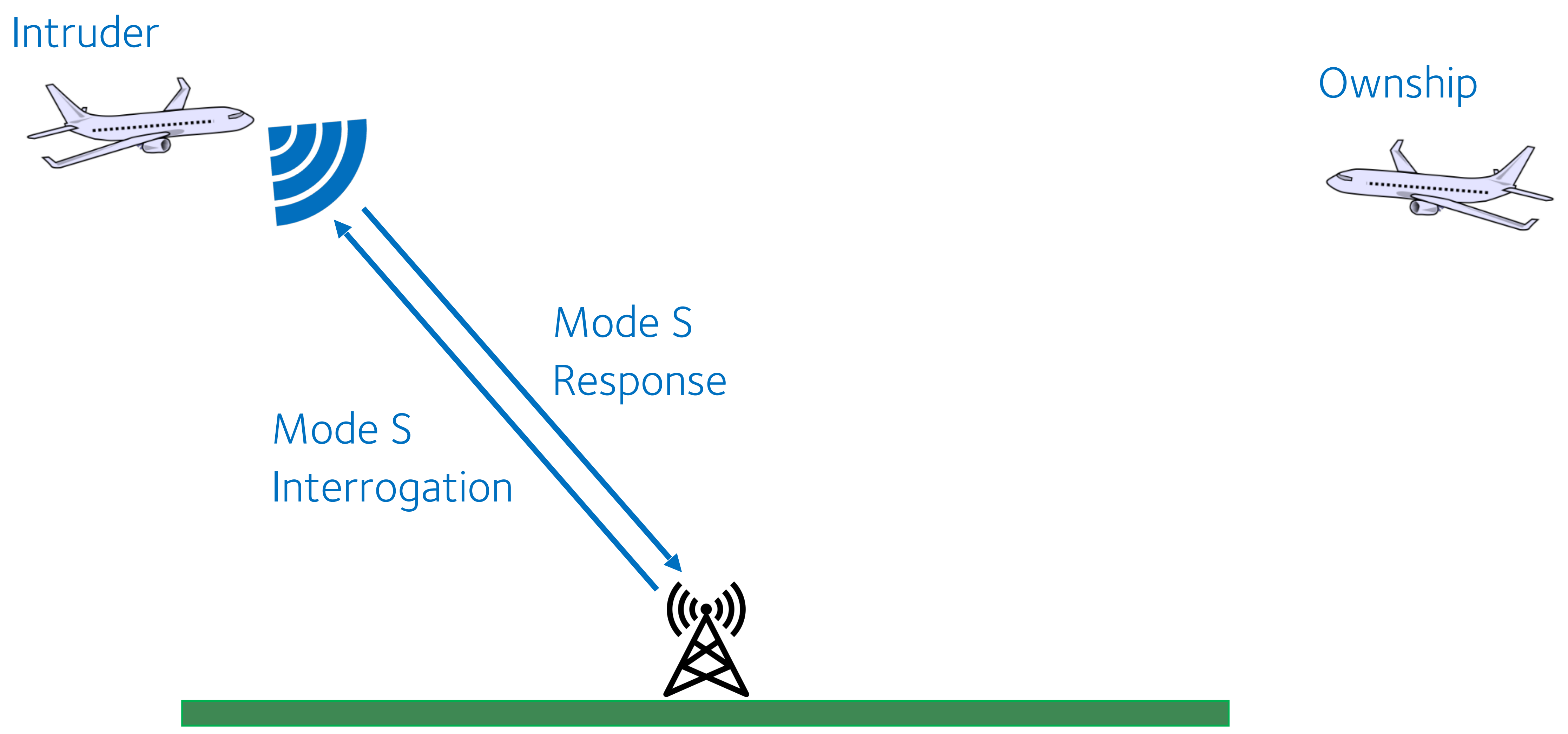
Traffic Collision Avoidance System

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters



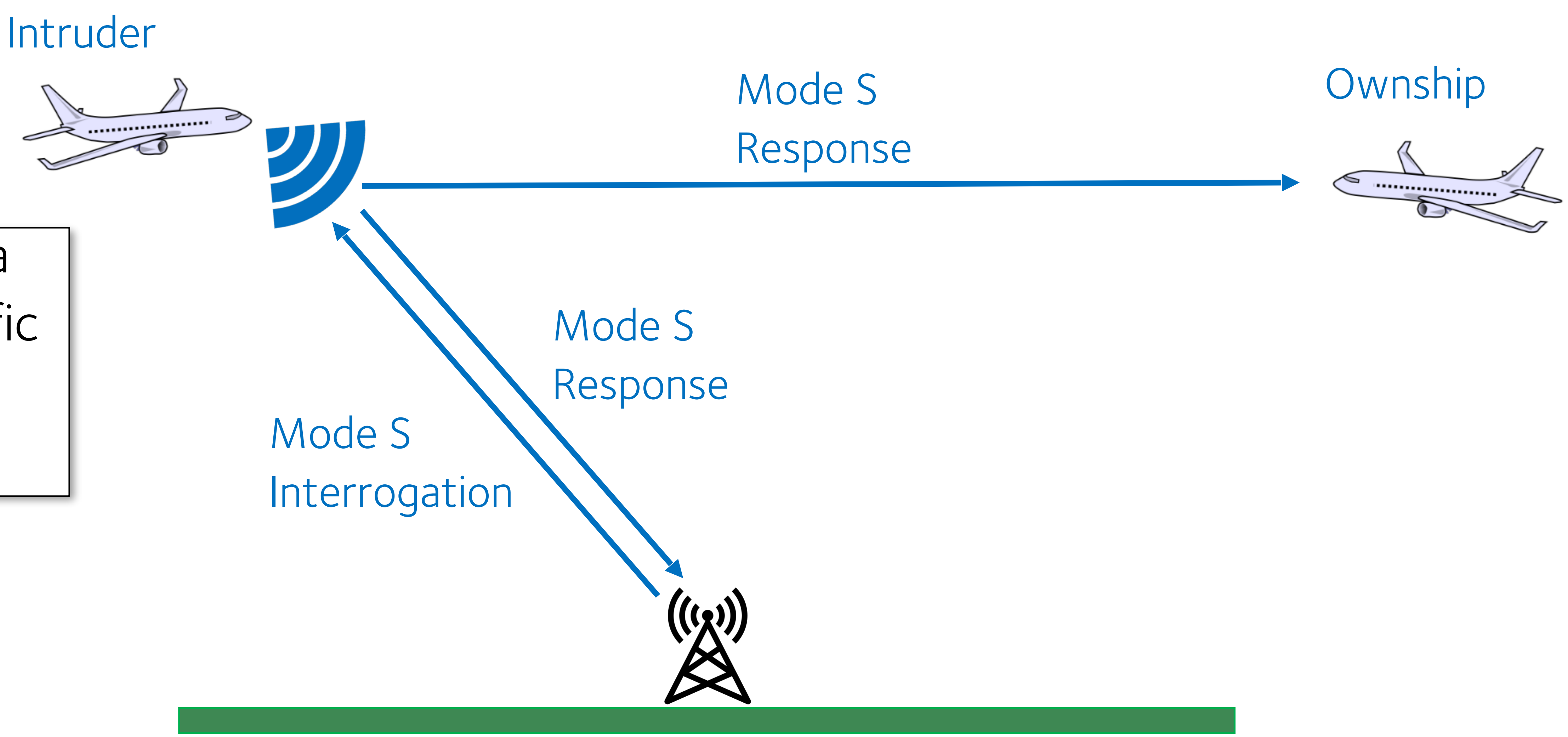
Traffic Collision Avoidance System

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters



Traffic Collision Avoidance System

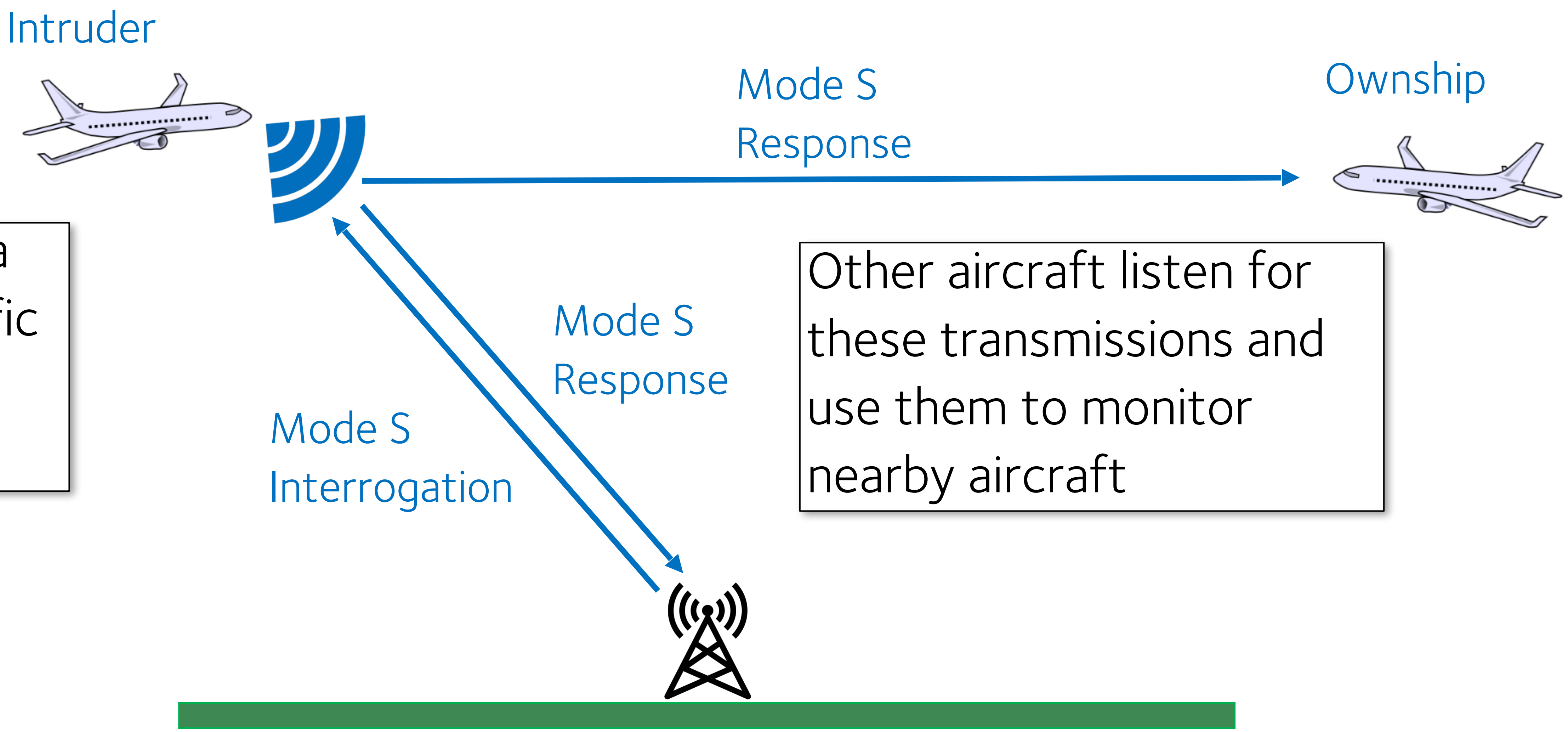
TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters



Aircraft transmit data requested by air traffic control data to the ground via Mode S

Traffic Collision Avoidance System

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters



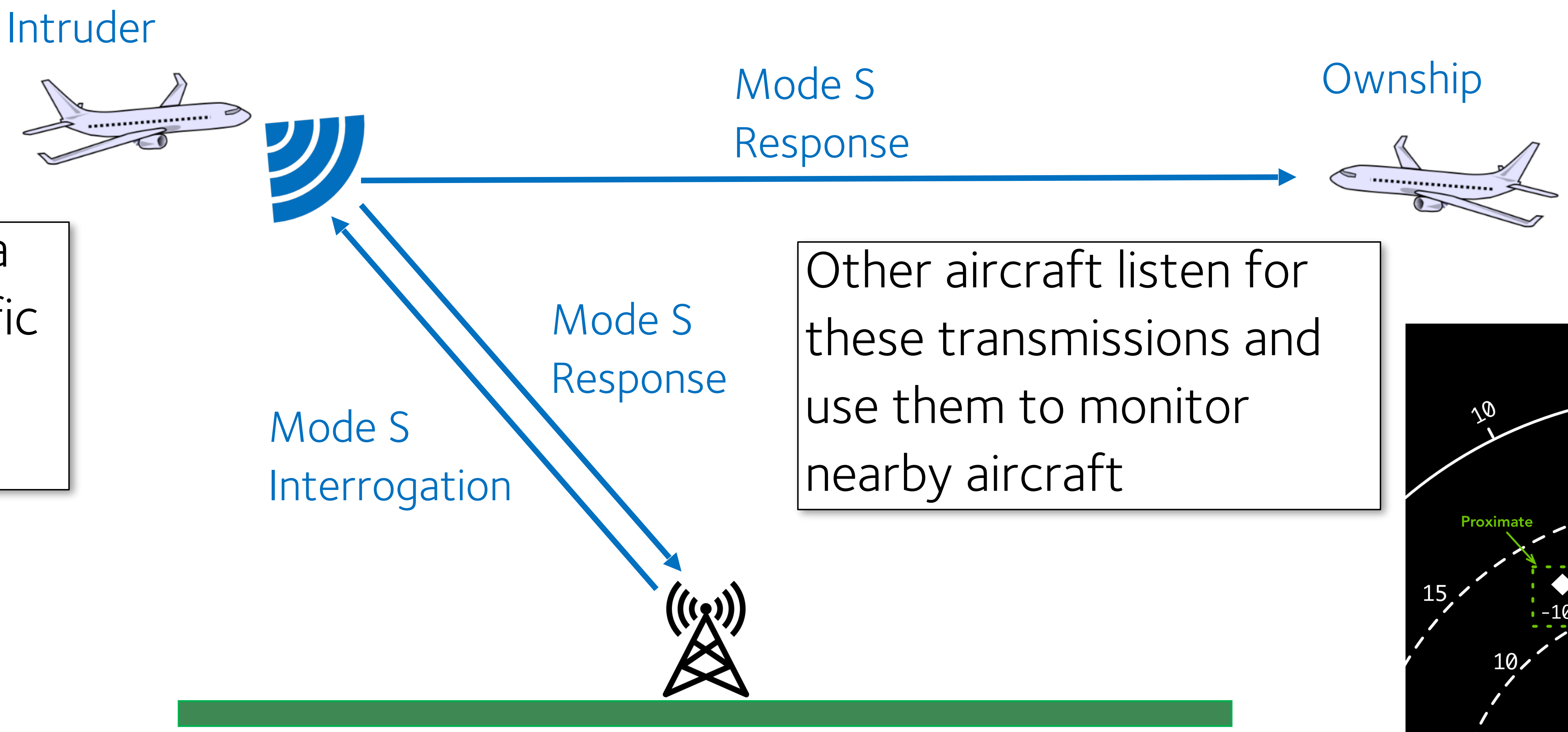
Aircraft transmit data requested by air traffic control data to the ground via Mode S

Other aircraft listen for these transmissions and use them to monitor nearby aircraft

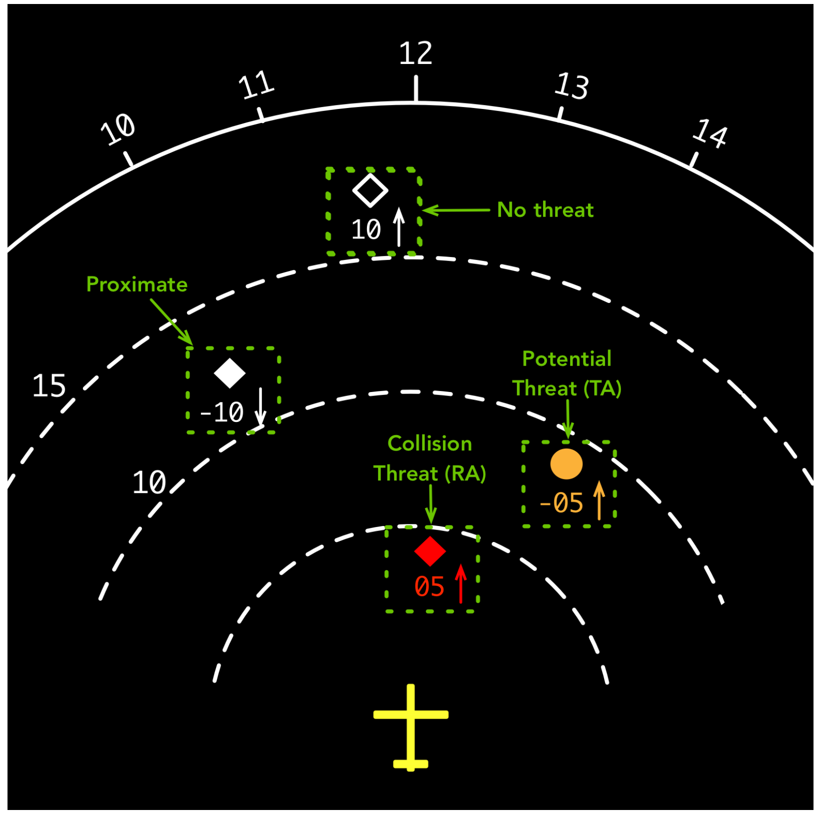
TRAFFIC COLLISION AVOIDANCE SYSTEM

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters

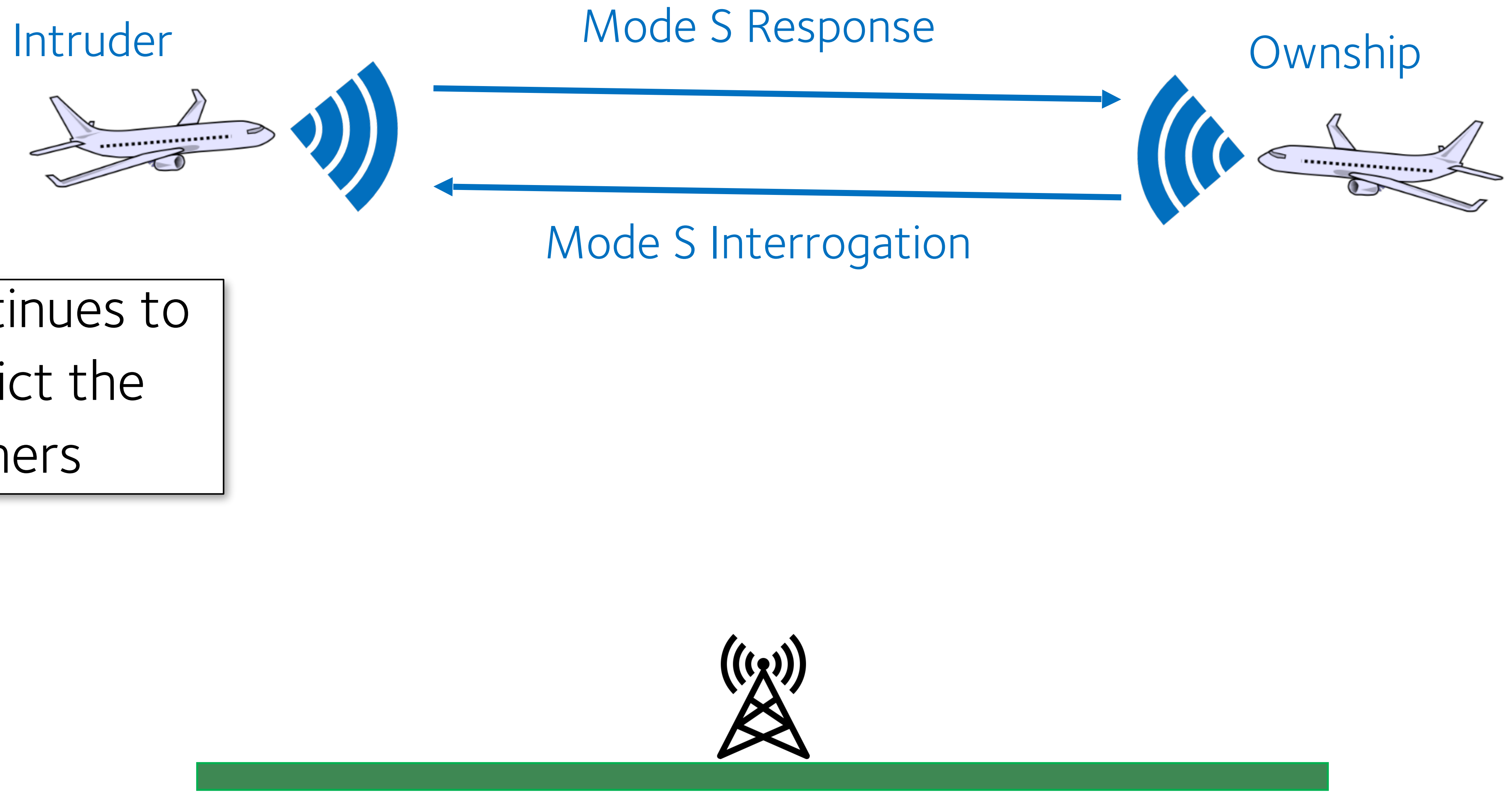
Aircraft transmit data requested by air traffic control data to the ground via Mode S



Other aircraft listen for these transmissions and use them to monitor nearby aircraft

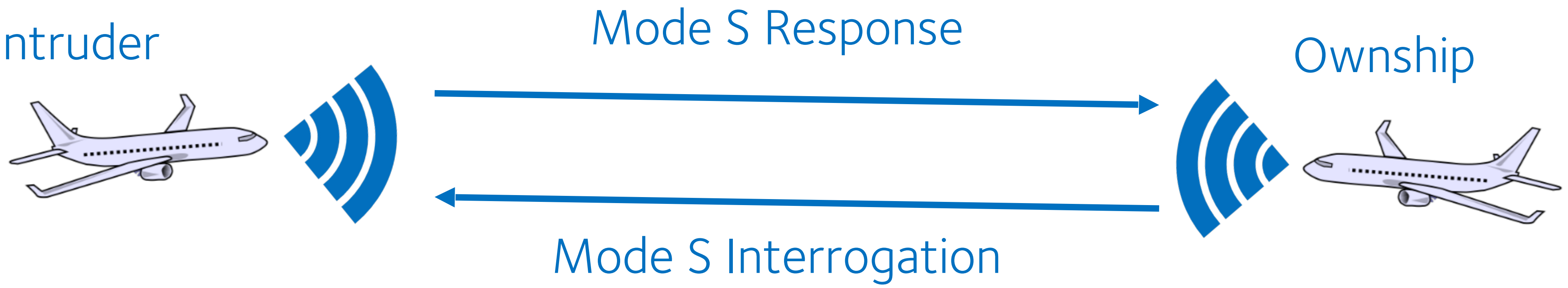


Traffic Collision Avoidance System



As each aircraft continues to move, they will predict the flight path of the others

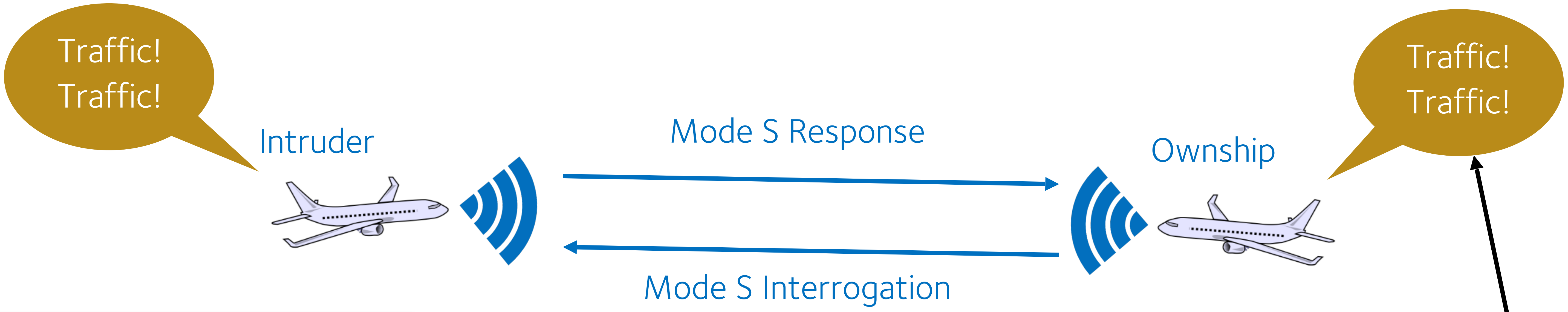
TRAFFIC COLLISION AVOIDANCE SYSTEM



As each aircraft continues to move, they will predict the flight path of the others

If the flight paths suggest the aircraft are too close, but not yet a risk, a Traffic Advisory (TA) will be issued

Traffic Collision Avoidance System

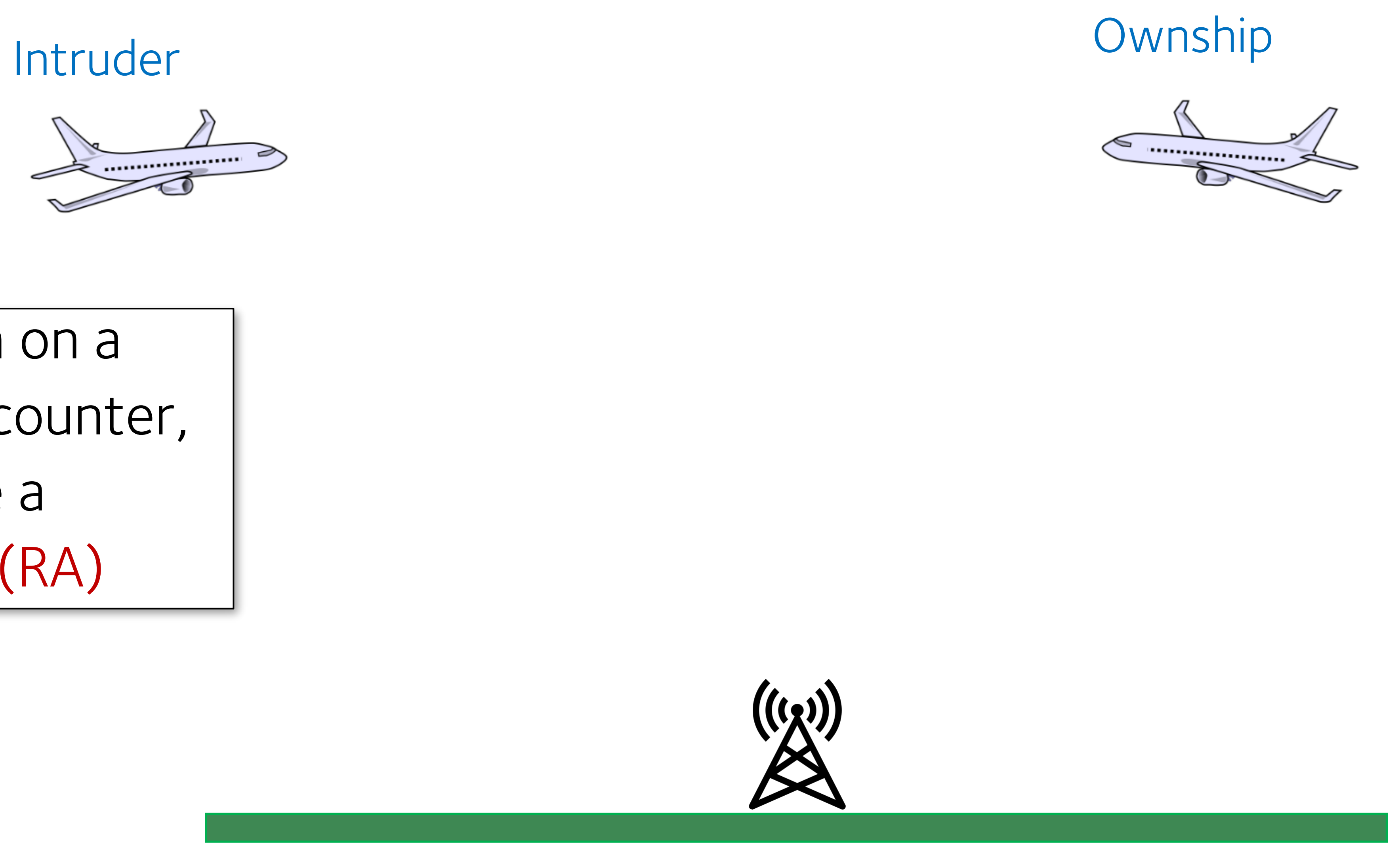


As each aircraft continues to move, they will predict the flight path of the others

If the flight paths suggest the aircraft are too close, but not yet a risk, a Traffic Advisory (TA) will be issued

This will be announced in the cockpit automatically

Traffic Collision Avoidance System



If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

Traffic Collision Avoidance System

If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

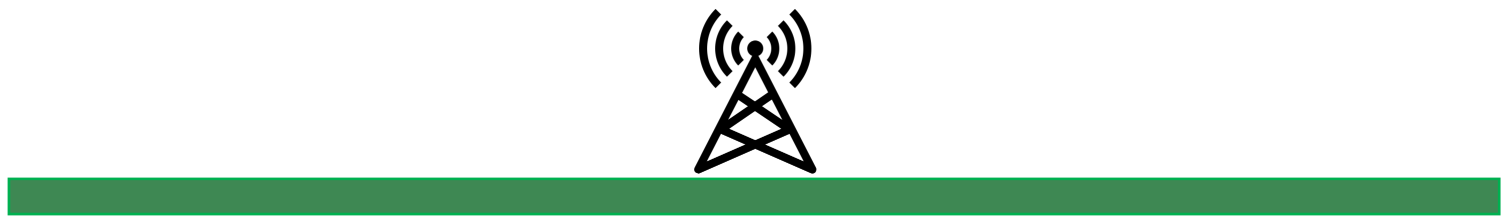
The aircraft will communicate to coordinate their planned RA movements

Traffic Collision Avoidance System

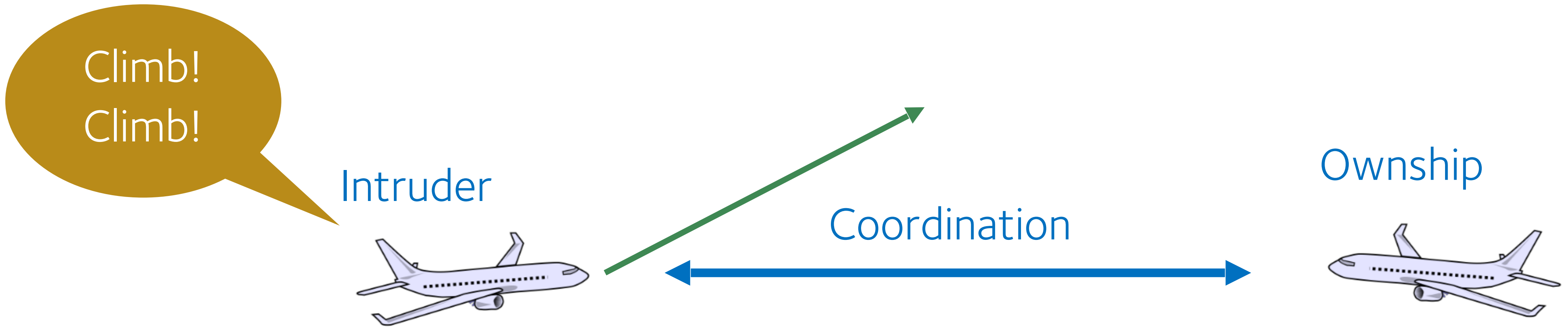
If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

The aircraft will communicate to coordinate their planned RA movements

The RAs will be announced in-cockpit as compulsory instructions



Traffic Collision Avoidance System

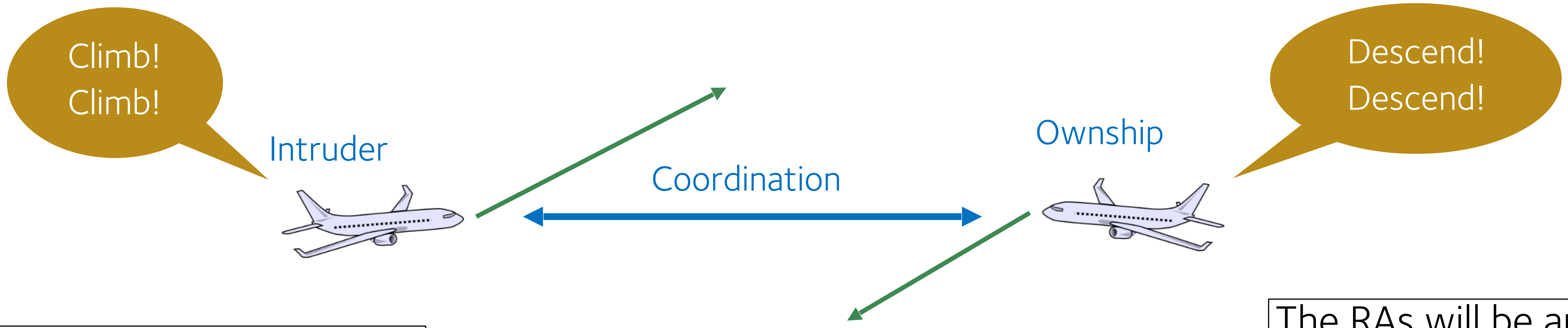


If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

The aircraft will communicate to coordinate their planned RA movements

The RAs will be announced in-cockpit as compulsory instructions

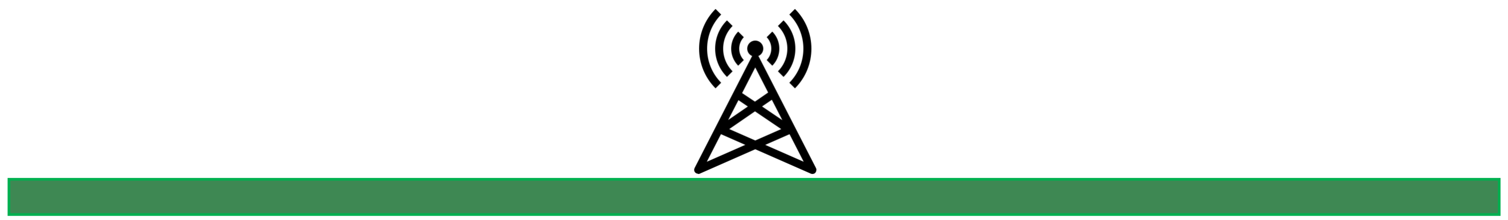
Traffic Collision Avoidance System



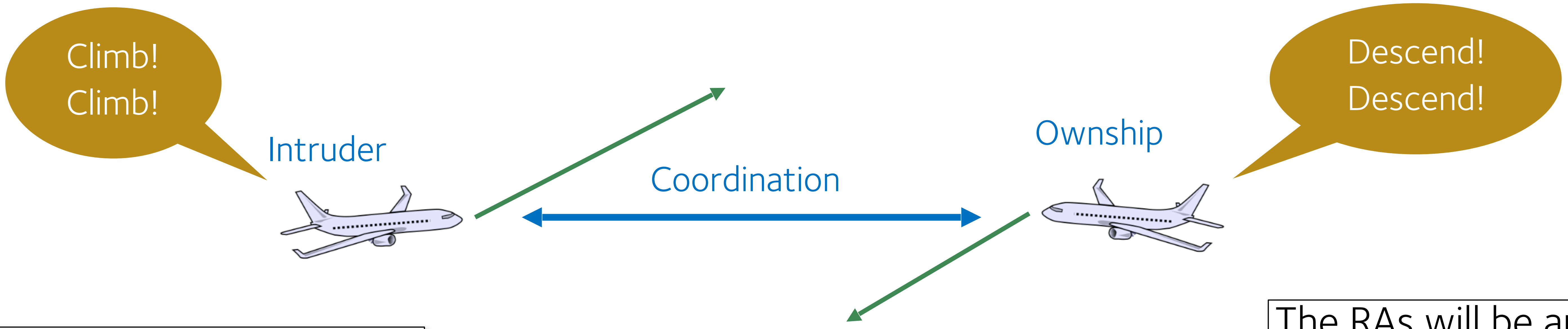
If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

The aircraft will communicate to coordinate their planned RA movements

The RAs will be announced in-cockpit as compulsory instructions



Traffic Collision Avoidance System



If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

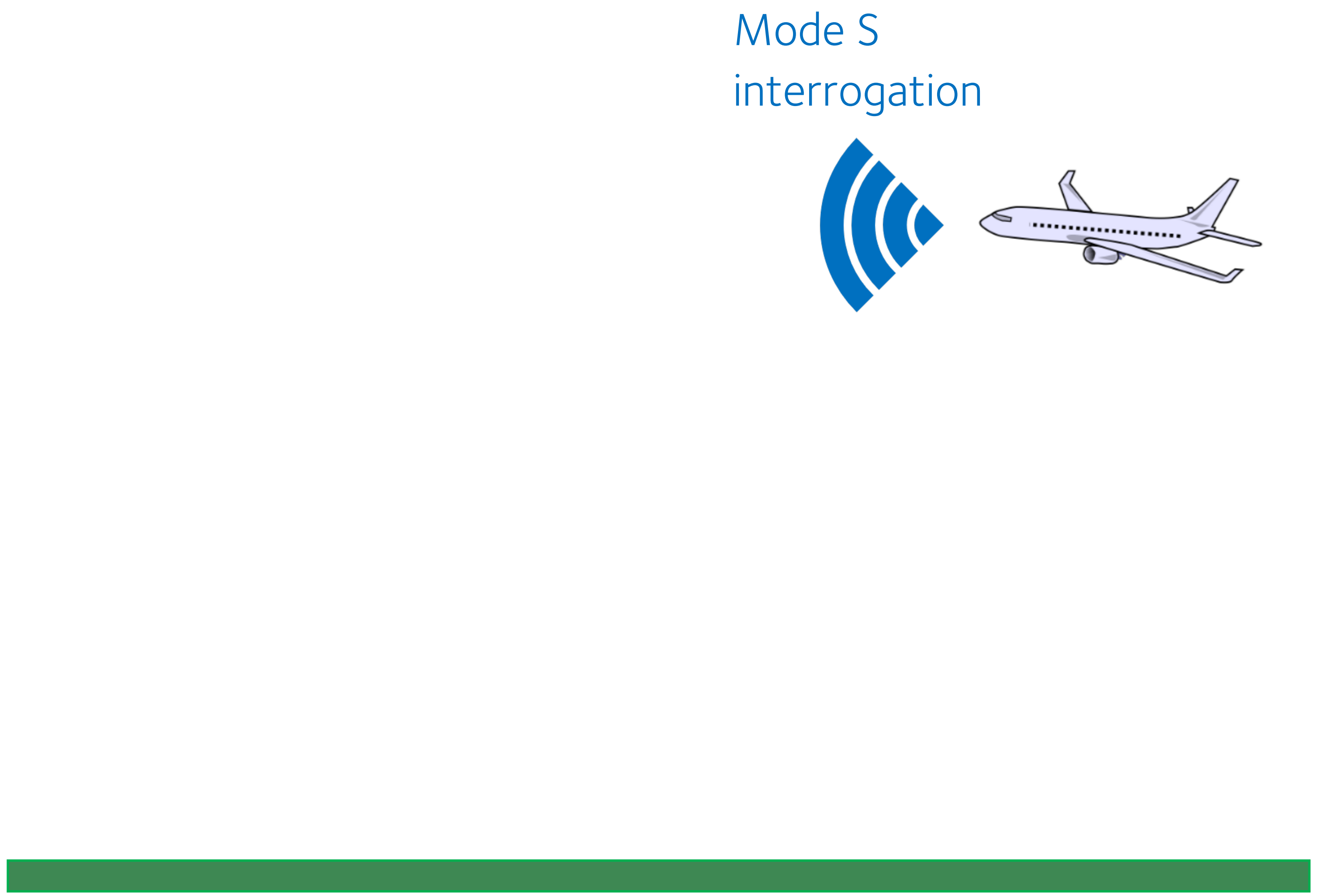
The aircraft will communicate to coordinate their planned RA movements

The RAs will be announced in-cockpit as compulsory instructions

TCAS procedure broadly expects aircraft to be cooperative

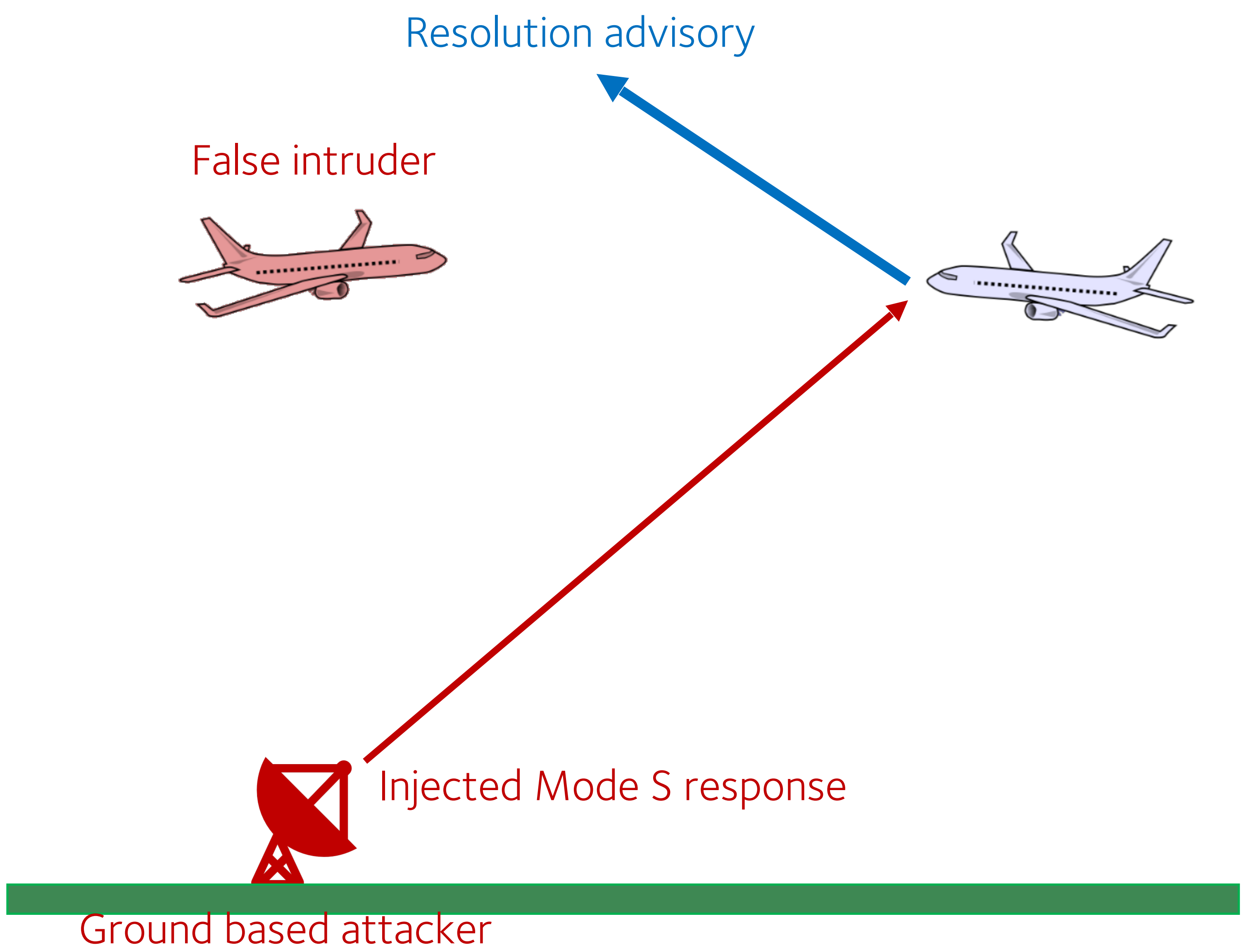
TCAS – Attack

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]



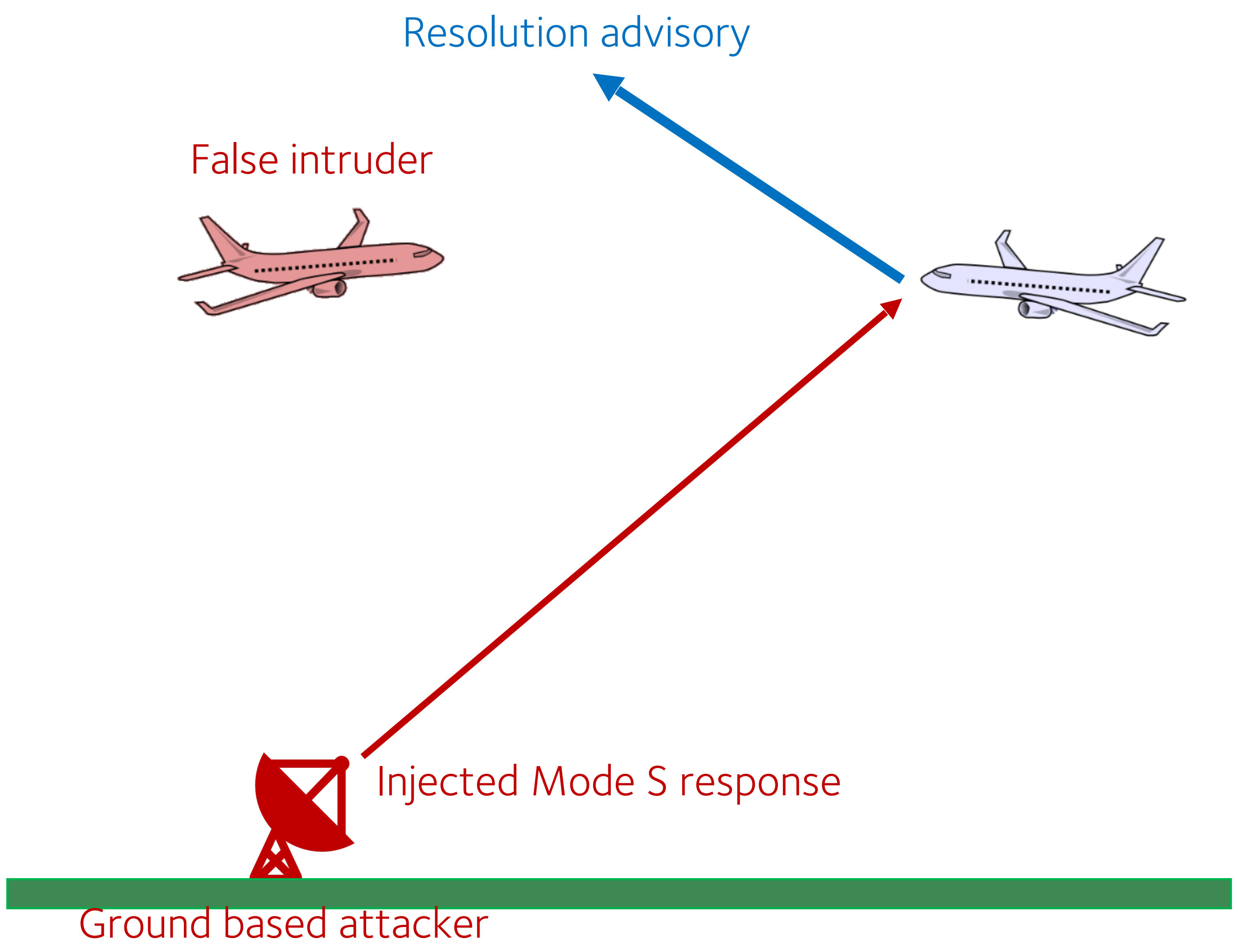
TCAS – ATTACK

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
- Attacker listens for Mode S interrogations issued by the aircraft and responds
    - Target aircraft believes an aircraft is flying towards it
    - Eventually this will cause a TA then RA, requiring avoiding action



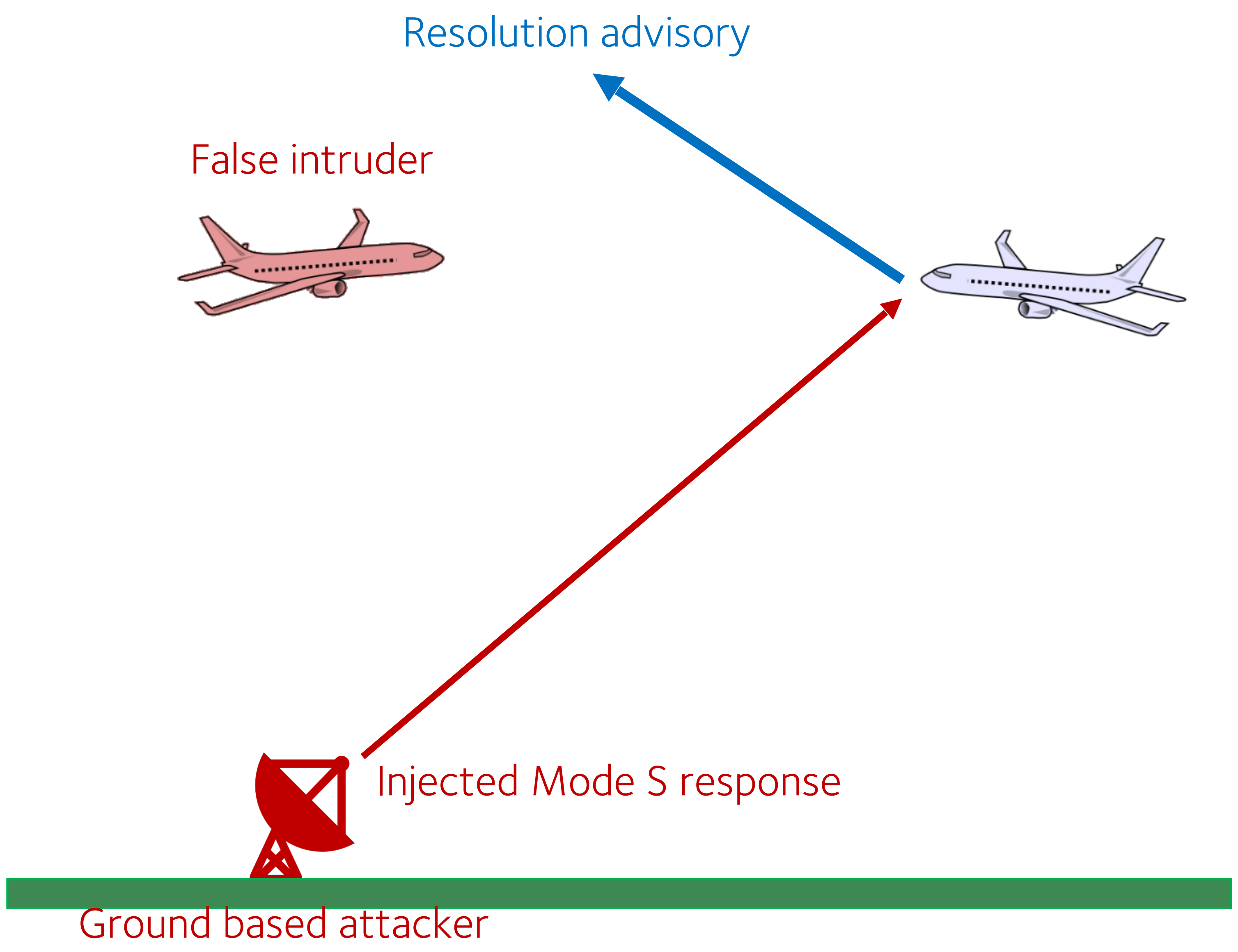
TCAS – Attack

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
- Attacker listens for Mode S interrogations issued by the aircraft and responds
  - Target aircraft believes an aircraft is flying towards it
  - Eventually this will cause a TA then RA, requiring avoiding action
- Simulator scenario saw the participant exposed to this multiple times in a flight



TCAS – Attack

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
- Attacker listens for Mode S interrogations issued by the aircraft and responds
    - Target aircraft believes an aircraft is flying towards it
    - Eventually this will cause a TA then RA, requiring avoiding action
- Simulator scenario saw the participant exposed to this multiple times in a flight



Aim: Force aircraft to repeatedly fly unwarranted Resolution Advisories

TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'
  - TA-Only after 4.5 RAs, Standby after a further 2.8 RAs

	Final Selected TCAS Mode			Total
	TA/RA	TA-Only	Standby	
Continue on route	4	10	8	22
Avoidance Maneuver	0	3	3	6
Divert to Origin	0	2	0	2
Total	4	15	11	30

TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'
  - TA-Only after 4.5 RAs, Standby after a further 2.8 RAs
  - Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden

	Final Selected TCAS Mode			Total
	TA/RA	TA-Only	Standby	
Continue on route	4	10	8	22
Avoidance Maneuver	0	3	3	6
Divert to Origin	0	2	0	2
Total	4	15	11	30

Effectively switching TCAS off

TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'
  - TA-Only after 4.5 RAs, Standby after a further 2.8 RAs
  - Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden
- Excess fuel burn in following RAs – but no choice

	Final Selected TCAS Mode			Total
	TA/RA	TA-Only	Standby	
Continue on route	4	10	8	22
Avoidance Maneuver	0	3	3	6
Divert to Origin	0	2	0	2
Total	4	15	11	30

Effectively switching TCAS off

TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'
  - TA-Only after 4.5 RAs, Standby after a further 2.8 RAs
  - Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden
- Excess fuel burn in following RAs – but no choice
- Most pilots continued on route but some felt the need to make extra maneuvers or divert

	Final Selected TCAS Mode			Total
	TA/RA	TA-Only	Standby	
Continue on route	4	10	8	22
Avoidance Maneuver	0	3	3	6
Divert to Origin	0	2	0	2
Total	4	15	11	30

TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'
  - TA-Only after 4.5 RAs, Standby after a further 2.8 RAs
  - Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden
- Excess fuel burn in following RAs – but no choice
- Most pilots continued on route but some felt the need to make extra maneuvers or divert
- Attacker can push pilots to fly unnecessary RAs and reduce TCAS sensitivity

	Final Selected TCAS Mode			Total
	TA/RA	TA-Only	Standby	
Continue on route	4	10	8	22
Avoidance Maneuver	0	3	3	6
Divert to Origin	0	2	0	2
Total	4	15	11	30

TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying

TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying

- Weather would have made attack identification much harder – cannot visually check

TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying

- Weather would have made attack identification much harder – cannot visually check
- Sudden, repeated RAs might have knock on effects for other aircraft

28 (93%) participants felt that this attack lowered the safety of the aircraft

TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying

- Weather would have made attack identification much harder – cannot visually check
- Sudden, repeated RAs might have knock on effects for other aircraft

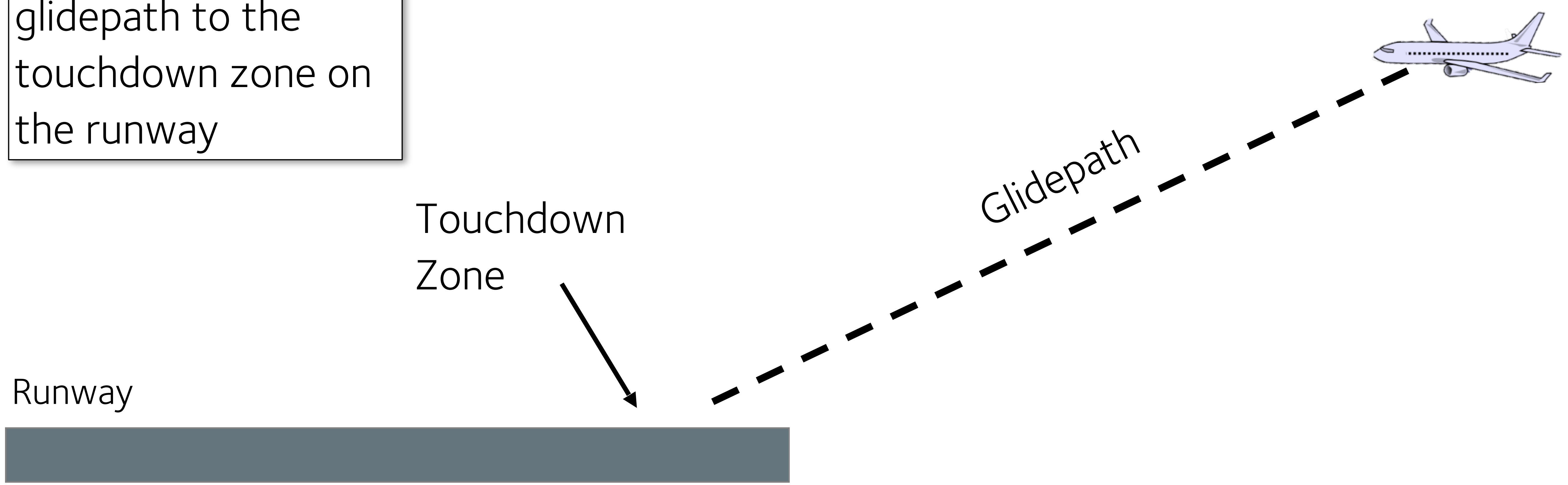
28 (93%) participants felt that this attack lowered the safety of the aircraft

- Pilots forced to reduce sensitivity of key safety system due to distraction

A participant highlighted a 'crying wolf' effect, which might impact future responses to TCAS

Instrument Landing System

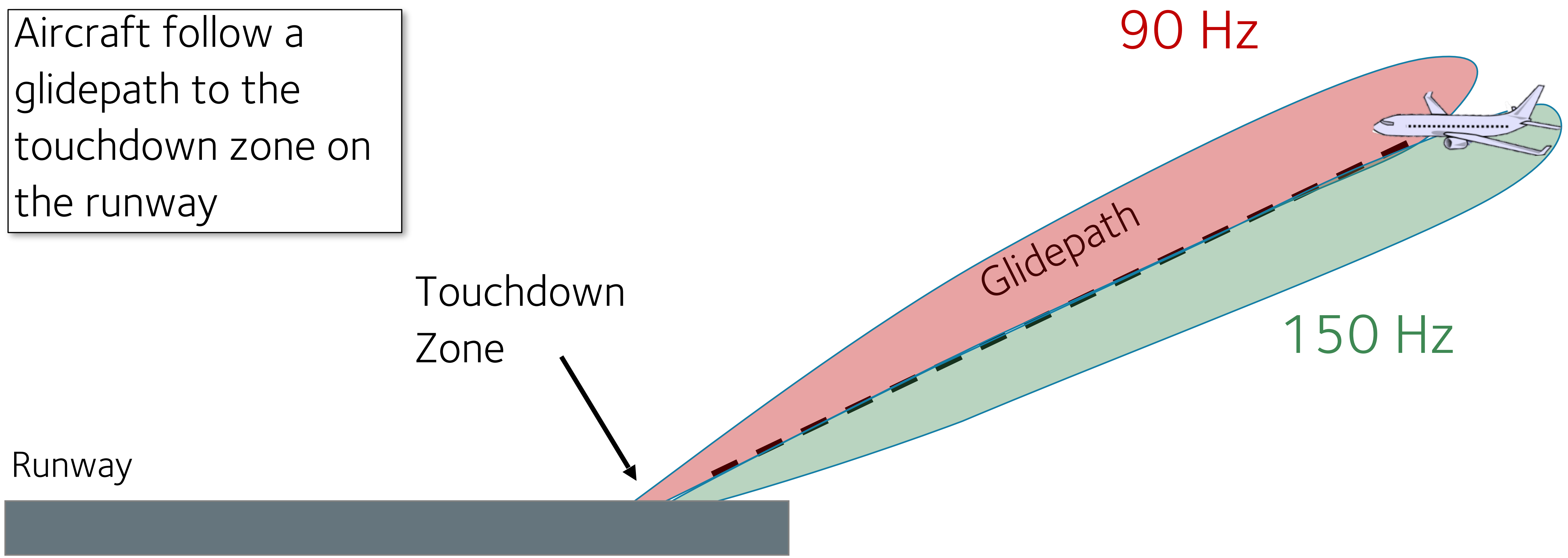
Aircraft follow a glidepath to the touchdown zone on the runway



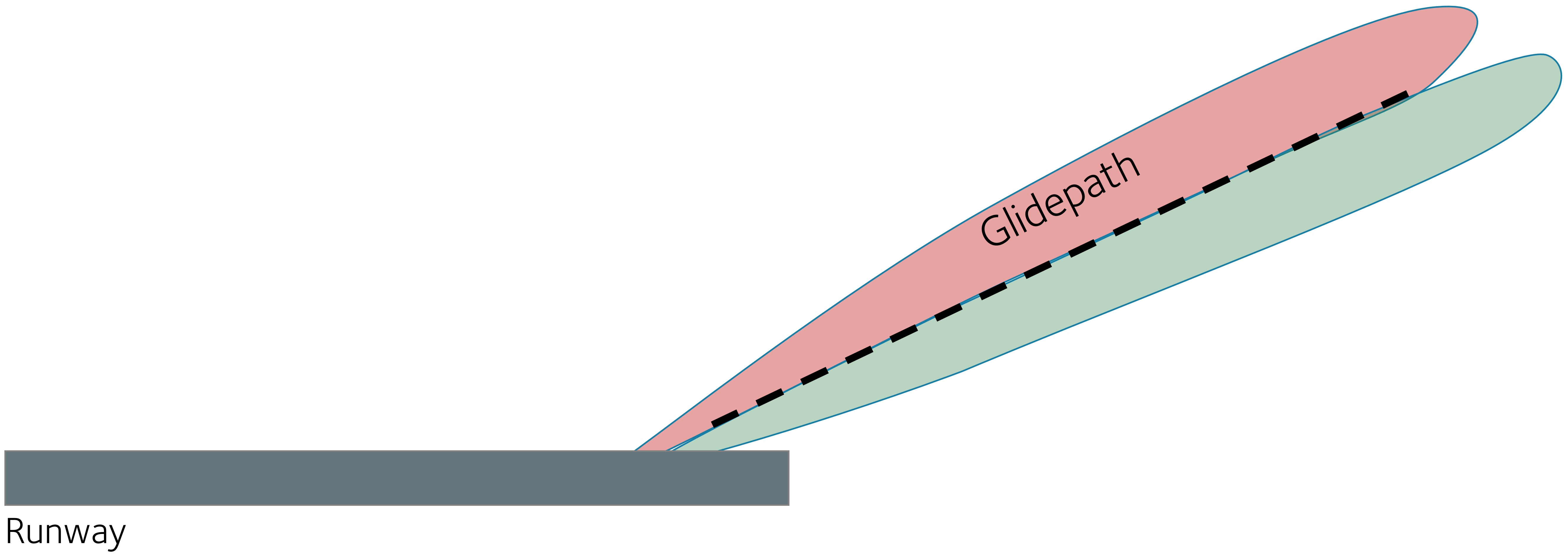
Instrument Landing System

Glideslope – a part of ILS – provides guidance along the ideal glidepath using overlapping lobes

Aircraft follow a glidepath to the touchdown zone on the runway

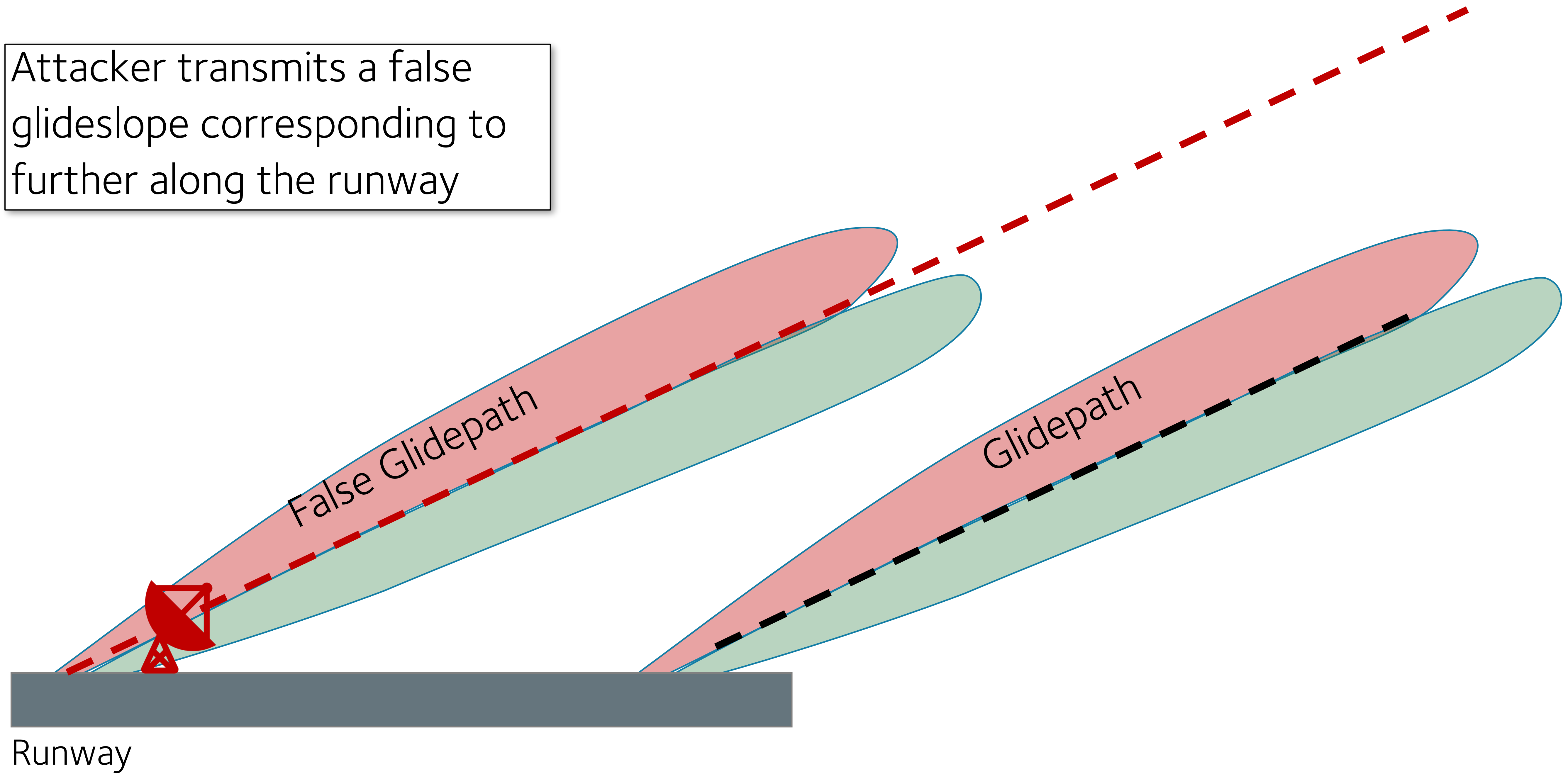


Glideslope – Attack

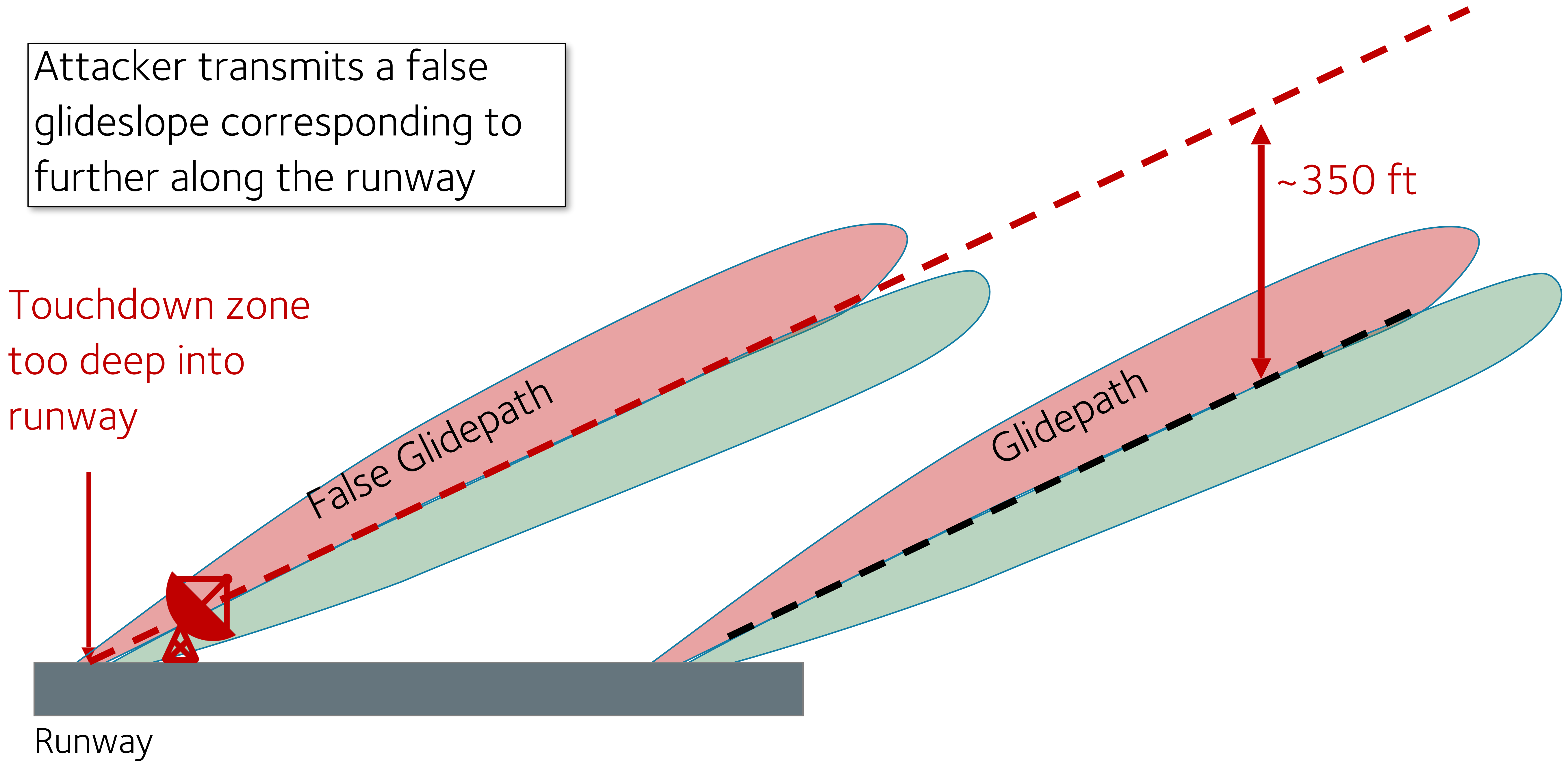


GLIDESLOPE – ATTACK

Attacker transmits a false glideslope corresponding to further along the runway

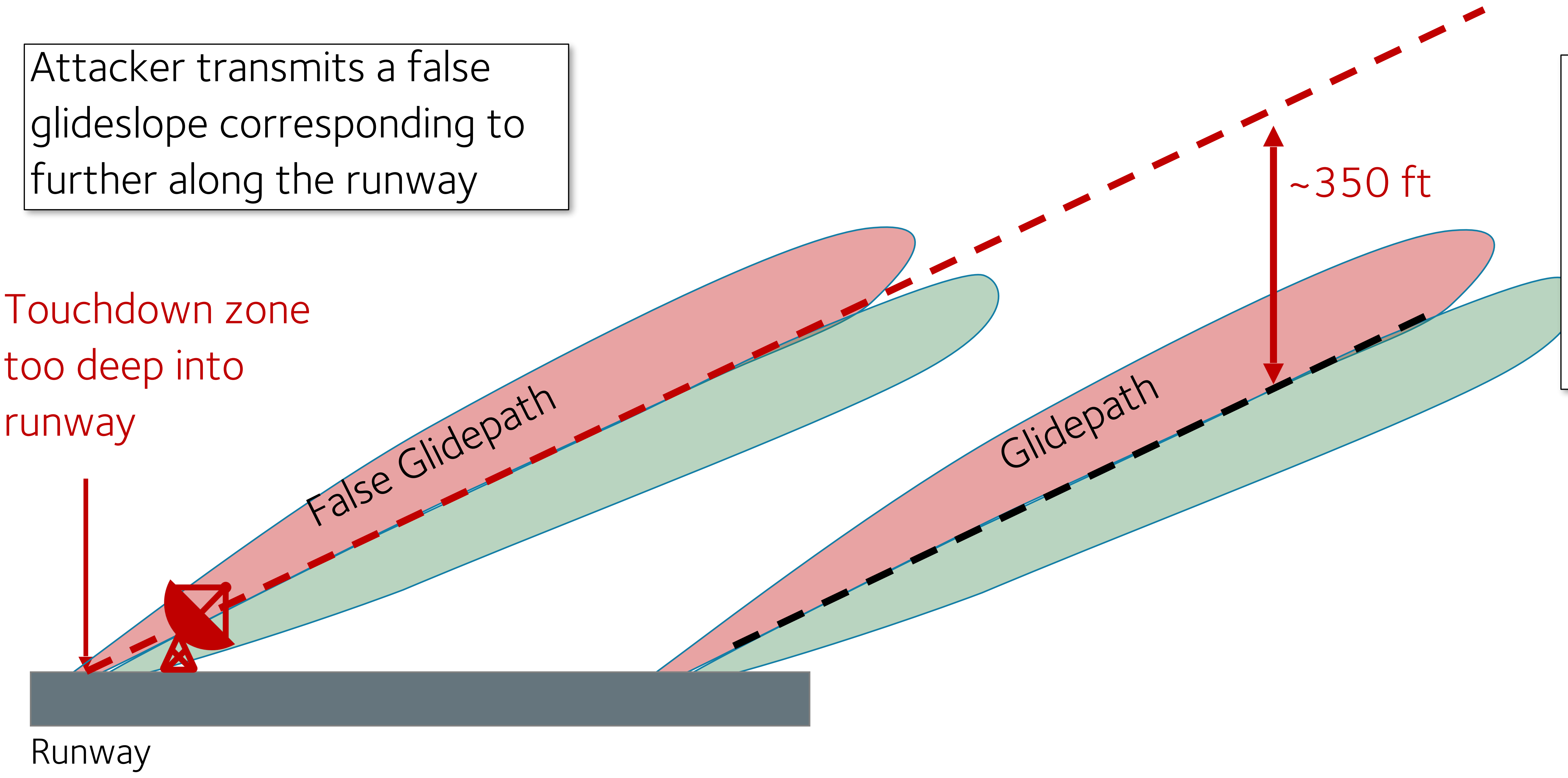


Glideslope – Attack



Glideslope – Attack

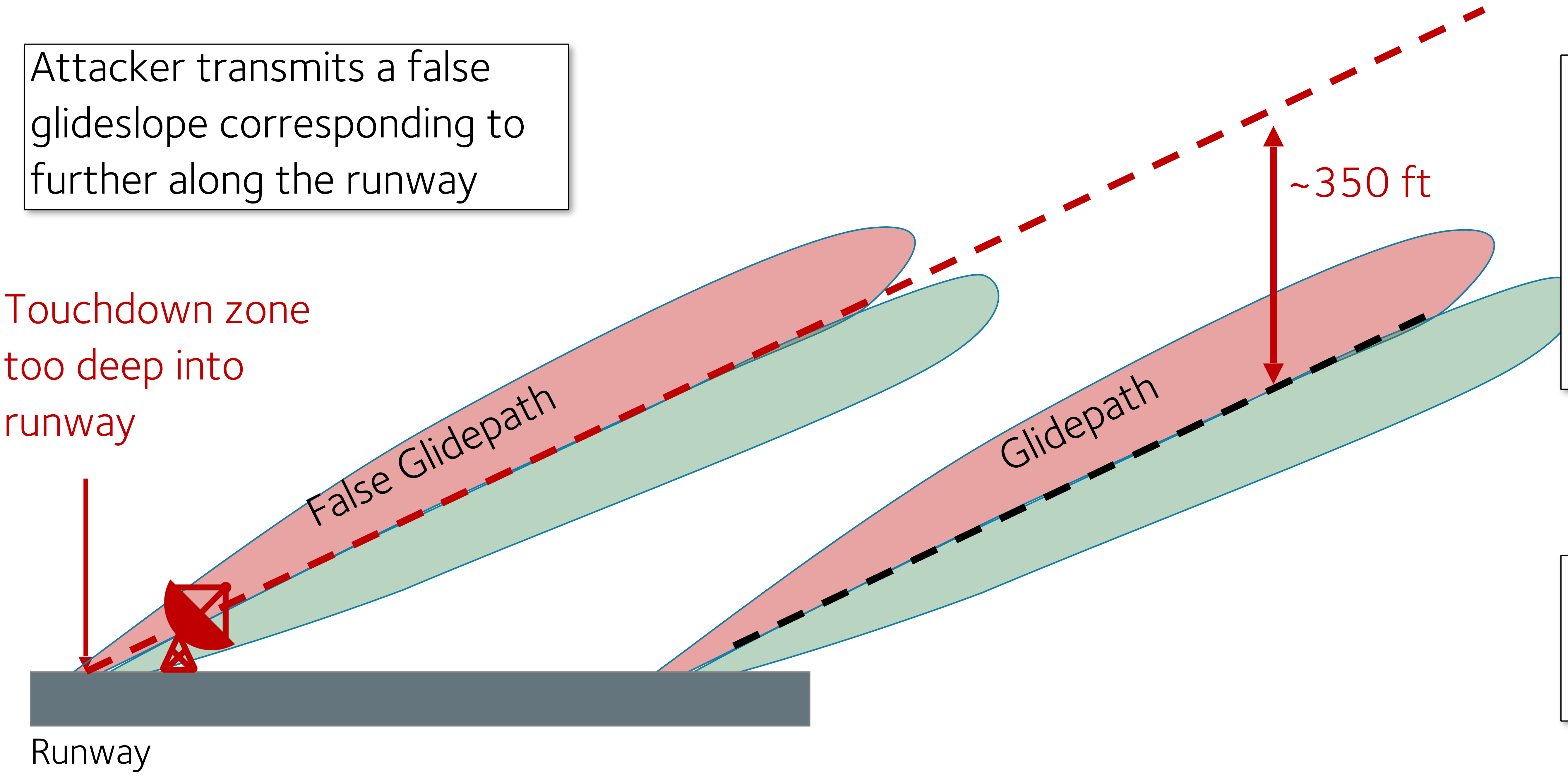
Attacker transmits a false glideslope corresponding to further along the runway



If the aircraft intercepts from above, or the attacker overpowers the real GS, the aircraft will follow the false GS

Glideslope – Attack

Attacker transmits a false glideslope corresponding to further along the runway

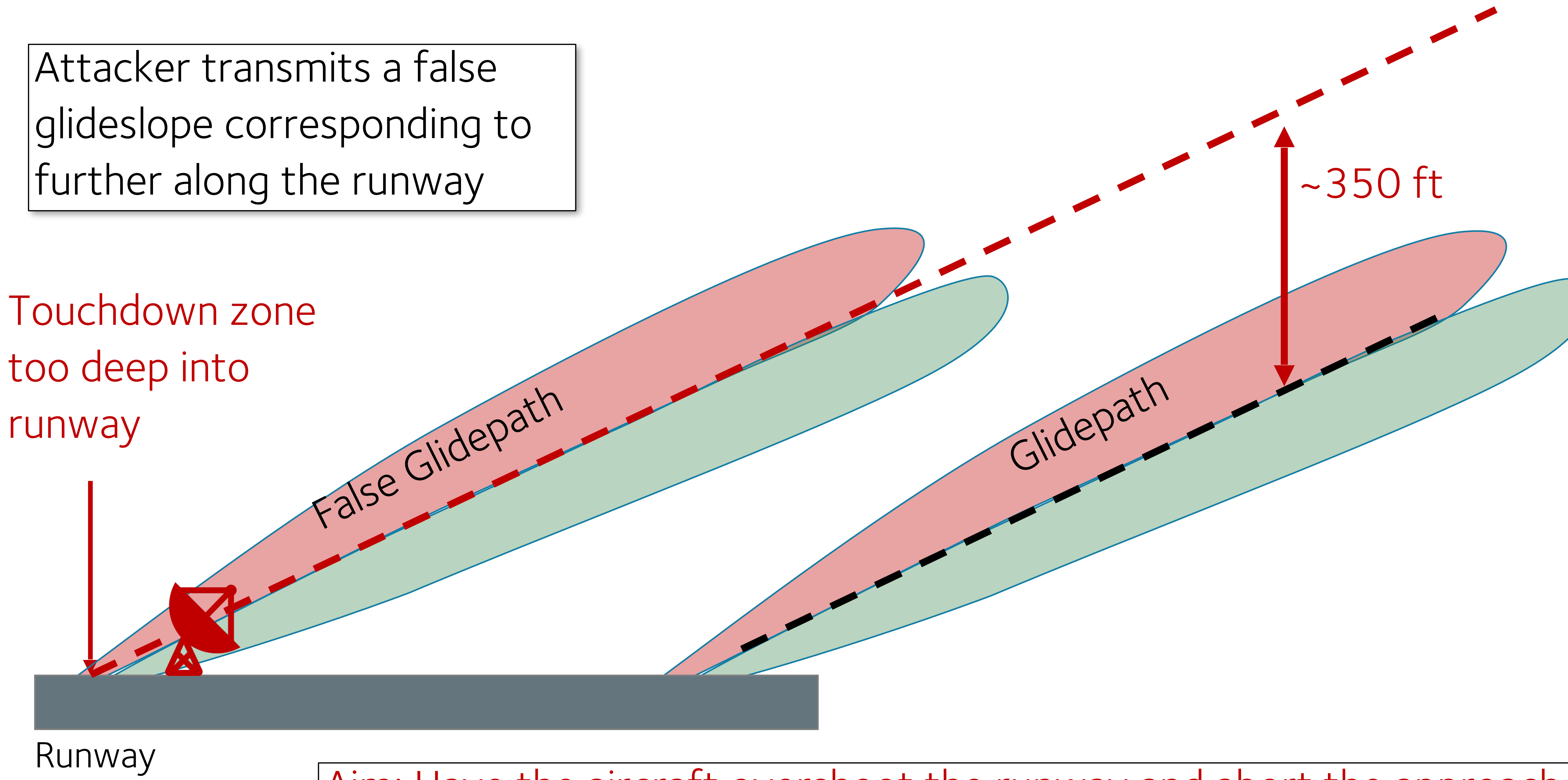


If the aircraft intercepts from above, or the attacker overpowers the real GS, the aircraft will follow the false GS

Similar concept to Sathaye et. al., USENIX '19 [2]

GLIDESLOPE – ATTACK

Attacker transmits a false glideslope corresponding to further along the runway



If the aircraft intercepts from above, or the attacker overpowers the real GS, the aircraft will follow the false GS

Similar concept to Sathaye et. al., USENIX '19 [2]

Aim: Have the aircraft overshoot the runway and abort the approach or land deep

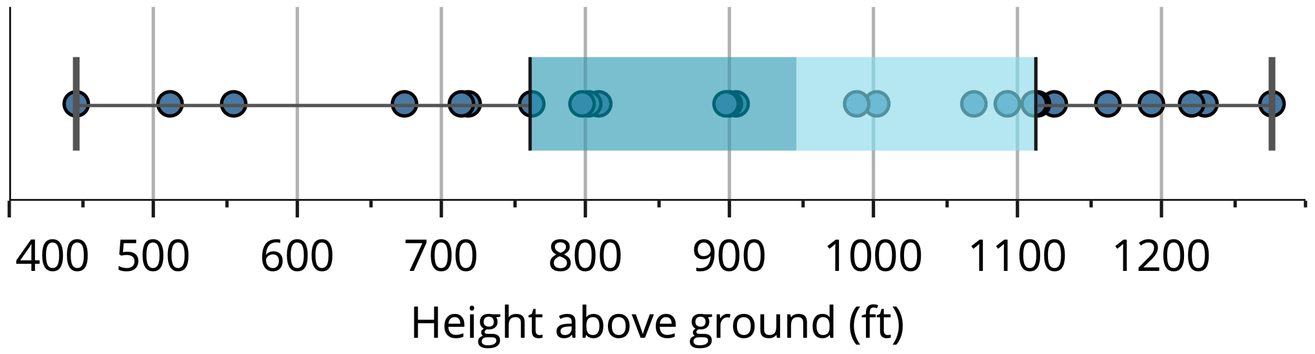
ILS/GS – Results

- Participants consistently identified a problem with ILS
  - 26 (87%) participants aborted their first approach
  - Subsequent approach methods avoided the glideslope, instead using different approaches methods

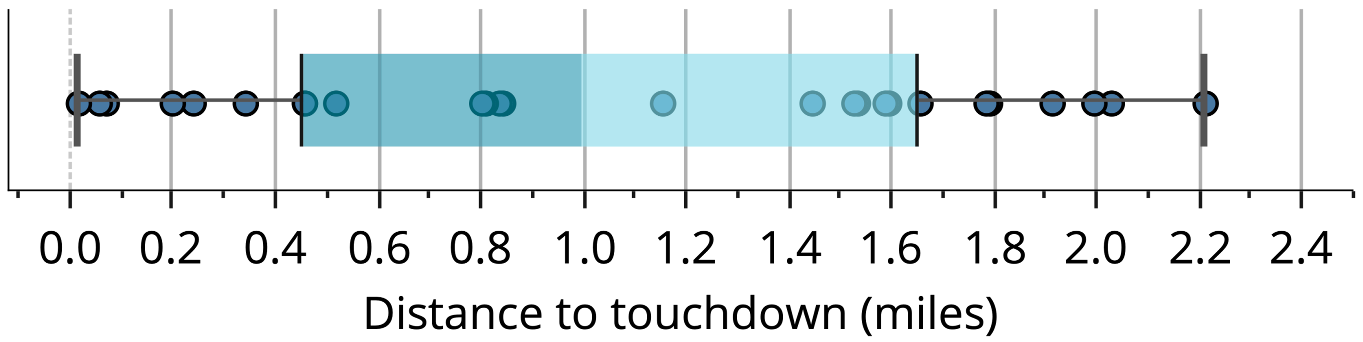
ILS/GS – Results

- Participants consistently identified a problem with ILS
  - 26 (87%) participants aborted their first approach
  - Subsequent approach methods avoided the glideslope, instead using different approaches methods
- Mean distance from touchdown at the point of go-around was 1.1 miles, at a height of 930 ft

Box plot of heights at the point of deciding to go around on the first approach



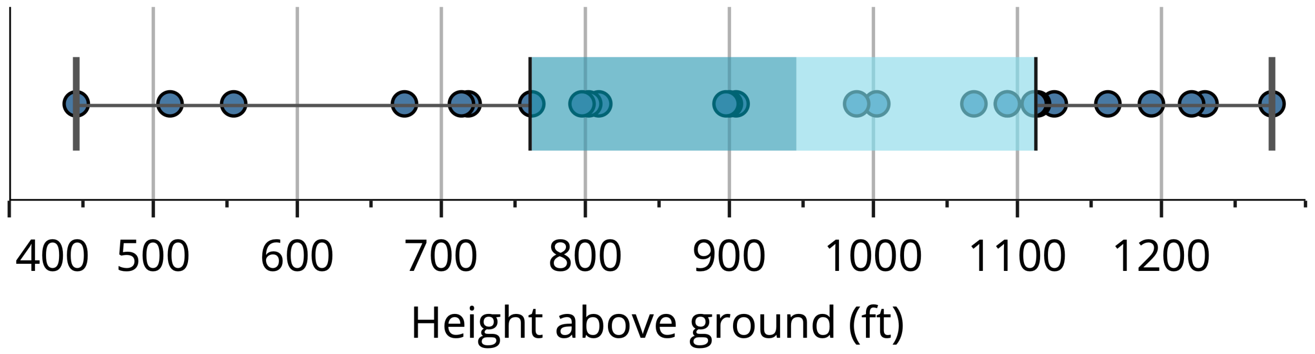
Distances from the runway touchdown zone at the point of deciding to go around on the first approach



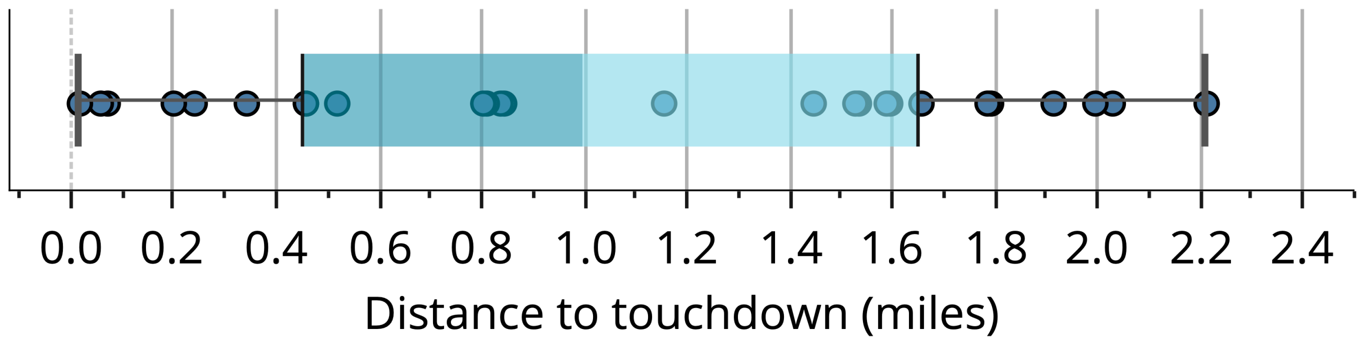
ILS/GS – Results

- Participants consistently identified a problem with ILS
  - 26 (87%) participants aborted their first approach
  - Subsequent approach methods avoided the glideslope, instead using different approaches methods
- Mean distance from touchdown at the point of go-around was 1.1 miles, at a height of 930 ft
- In the cases of landing on first approach, pilots had to make a steep correction – not always possible

Box plot of heights at the point of deciding to go around on the first approach



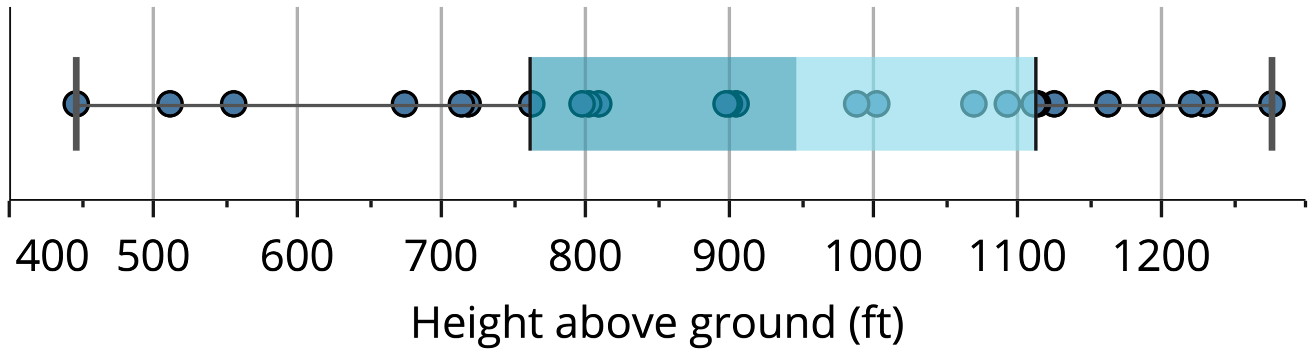
Distances from the runway touchdown zone at the point of deciding to go around on the first approach



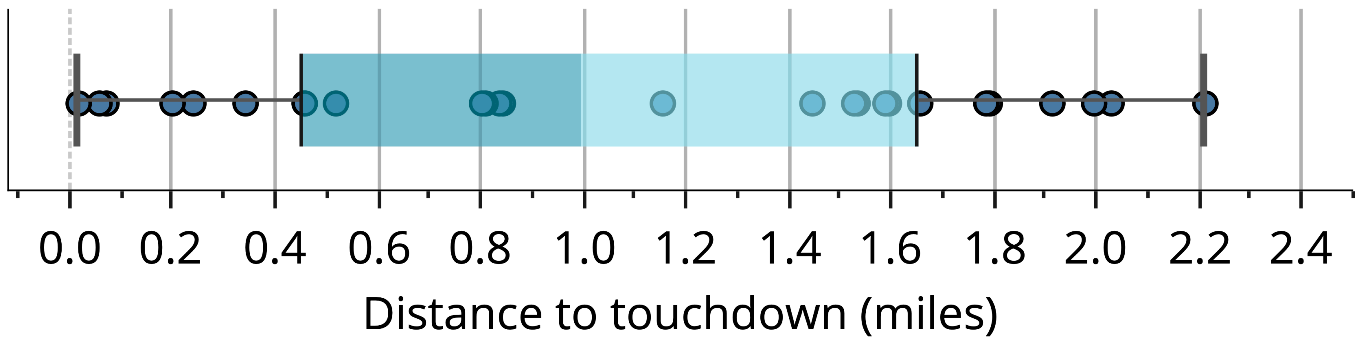
ILS/GS – Results

- Participants consistently identified a problem with ILS
  - 26 (87%) participants aborted their first approach
  - Subsequent approach methods avoided the glideslope, instead using different approaches methods
- Mean distance from touchdown at the point of go-around was 1.1 miles, at a height of 930 ft
- In the cases of landing on first approach, pilots had to make a steep correction – not always possible
- Attacker can push pilots to miss an approach and abandon the glideslope

Box plot of heights at the point of deciding to go around on the first approach



Distances from the runway touchdown zone at the point of deciding to go around on the first approach



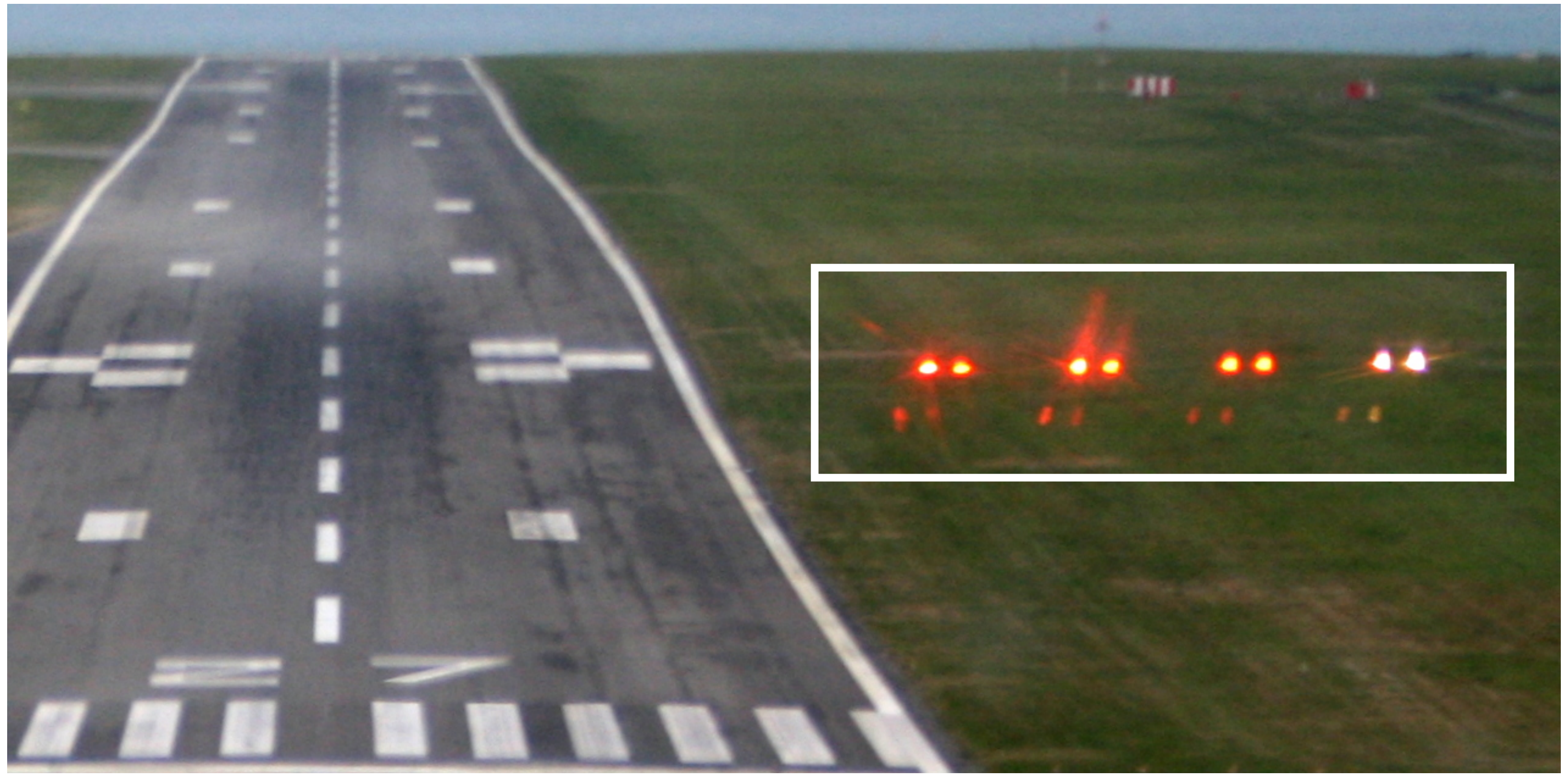
ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach

ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue

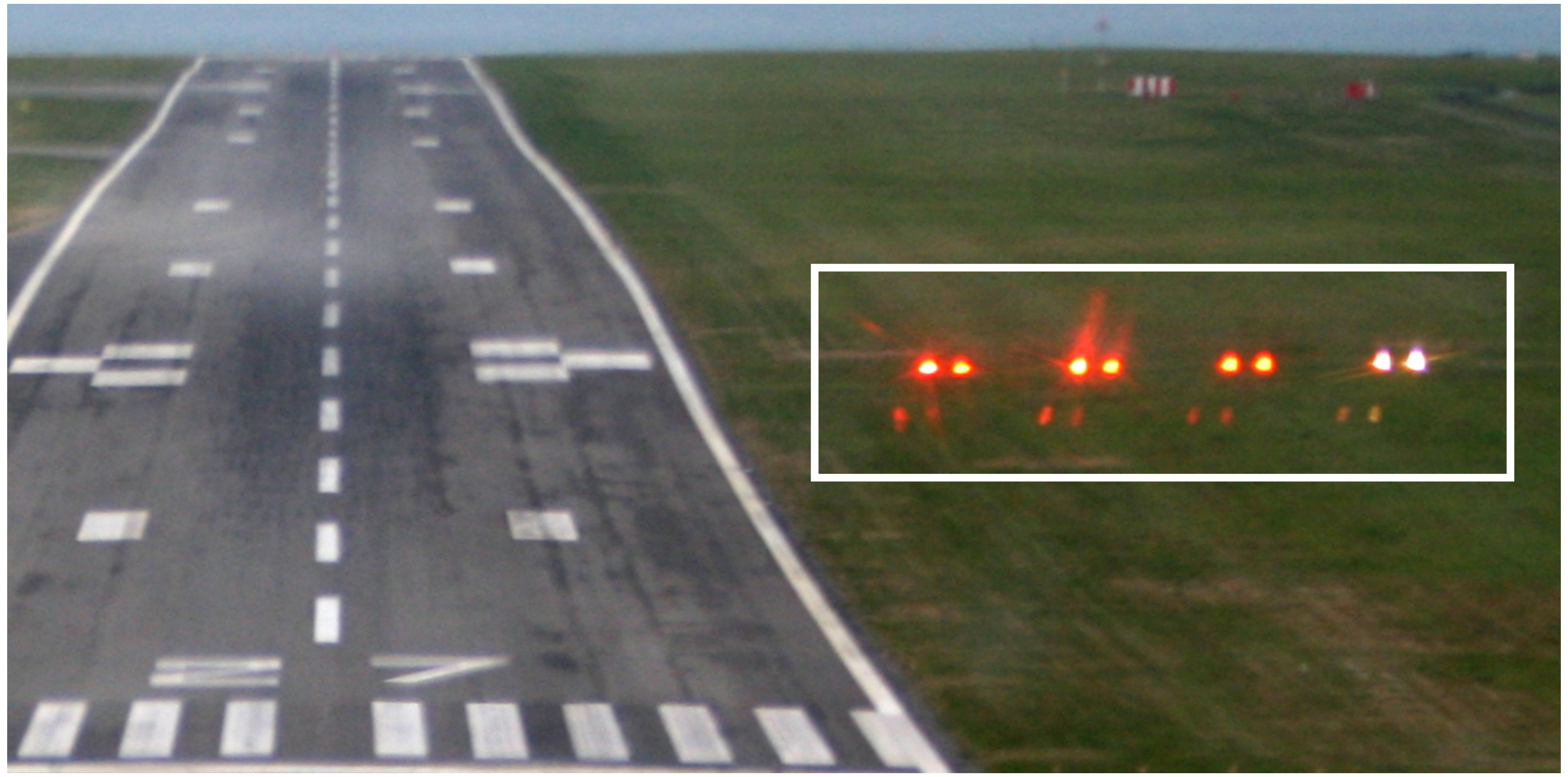
Precision Path Approach Indicators (PAPIs) [4]



ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue

Precision Path Approach Indicators (PAPIs) [4]

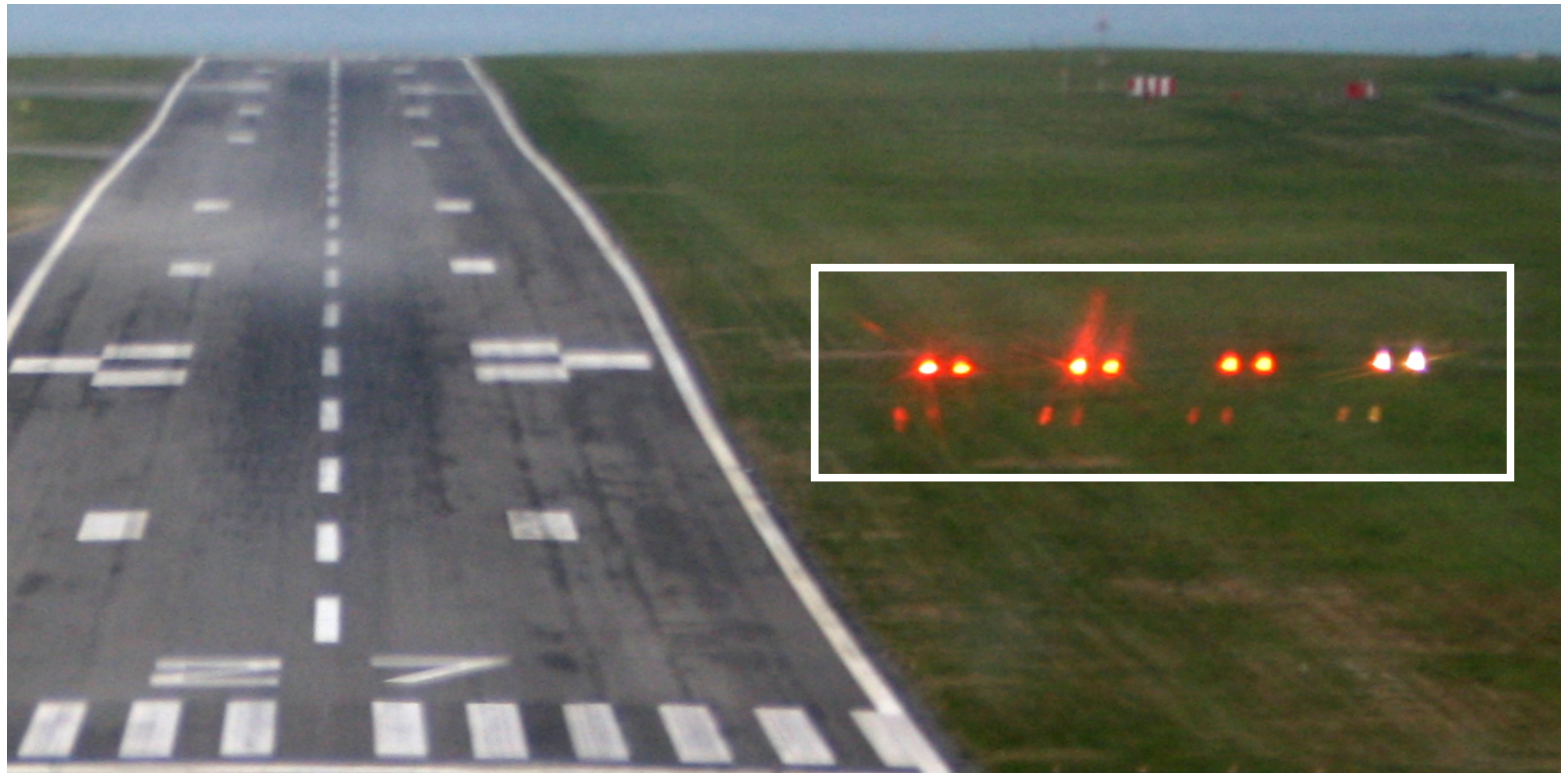


Participants noted that poor weather would have made this much harder to spot

ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue
- Much harder to manage in low-fuel situations

Precision Path Approach Indicators (PAPIs) [4]

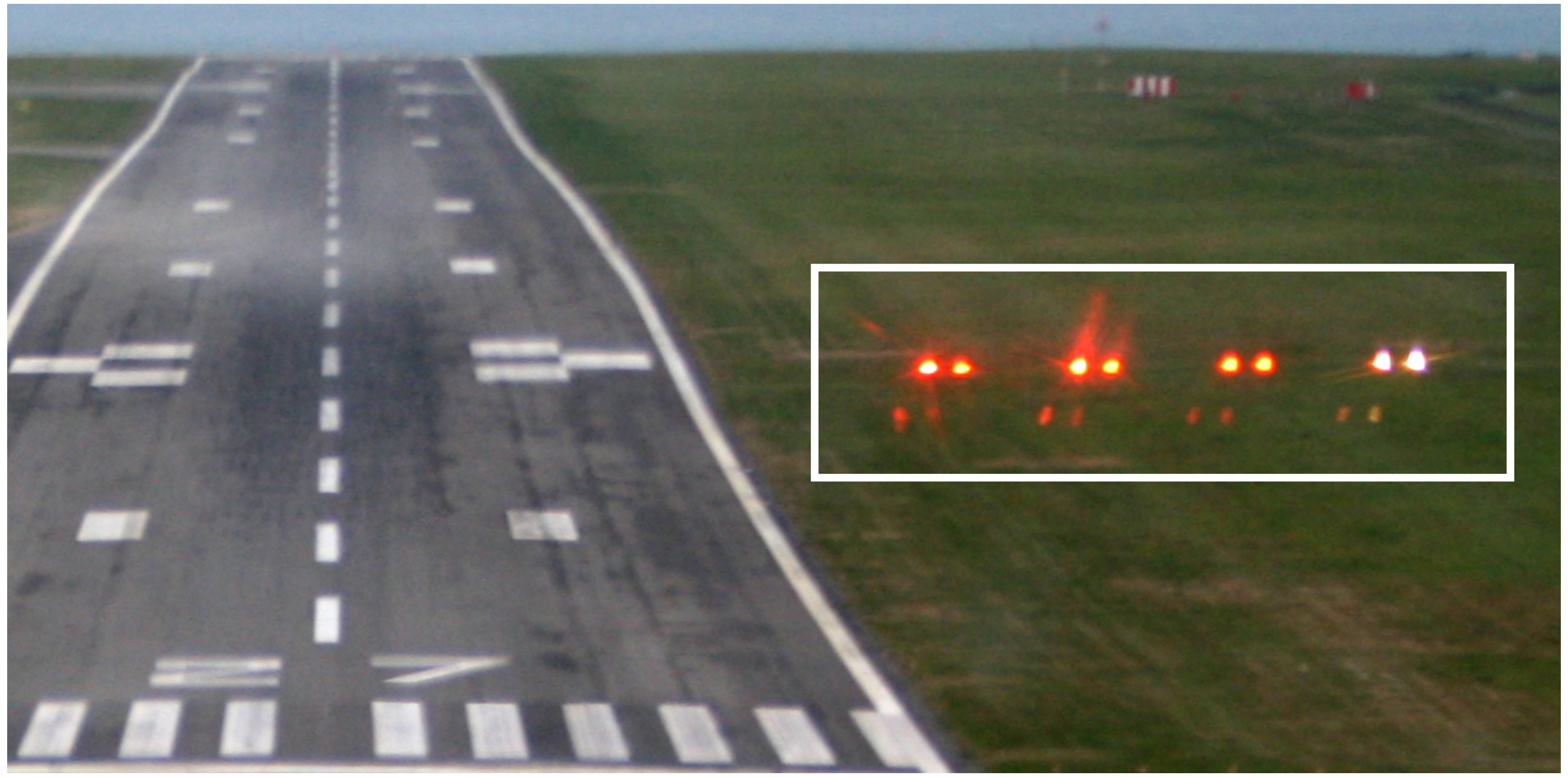


Participants noted that poor weather would have made this much harder to spot

ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue
- Much harder to manage in low-fuel situations
- Concern about a ‘short’ glideslope landing before the runway

Precision Path Approach Indicators (PAPIs) [4]

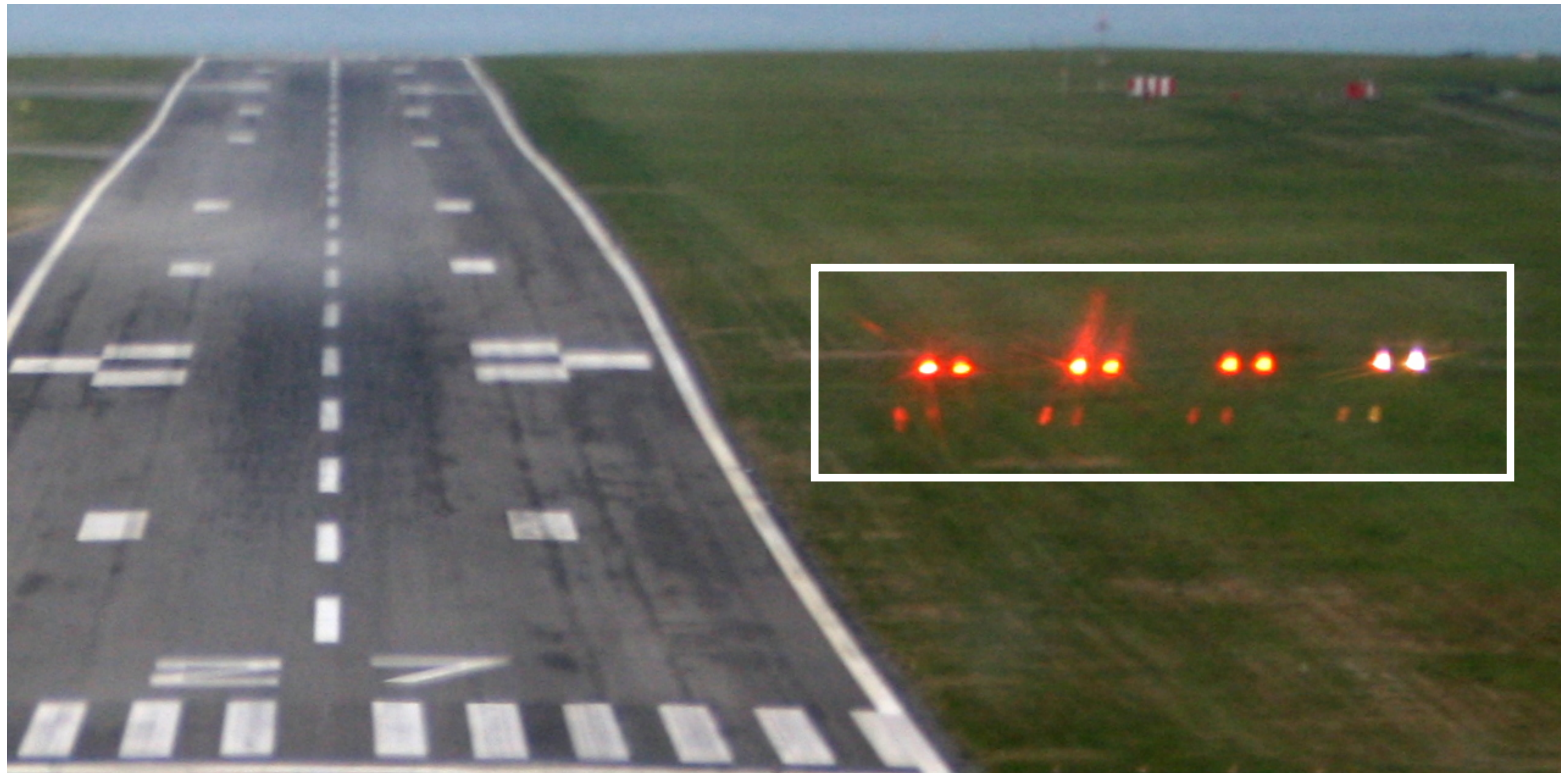


Participants noted that poor weather would have made this much harder to spot

ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue
- Much harder to manage in low-fuel situations
- Concern about a 'short' glideslope landing before the runway
- Wide range of second approach methods suggests uncertainty – though experience with GS oddities helps

Precision Path Approach Indicators (PAPIs) [4]



Participants noted that poor weather would have made this much harder to spot

General Findings

Observation

If attacks cause spurious alarms, the system will be turned off

Effect

General Findings

Observation

If attacks cause spurious alarms, the system will be turned off

Effect

Attackers 'force' pilots away from systems by attacking them

General Findings

Observation

If attacks cause spurious alarms, the system will be turned off

Attacks have real potential for disruption, though specific disruption is hard to predict

Effect

Attackers ‘force’ pilots away from systems by attacking them

General Findings

Observation

If attacks cause spurious alarms, the system will be turned off

Attacks have real potential for disruption, though specific disruption is hard to predict

Effect

Attackers 'force' pilots away from systems by attacking them

Can have a wider, more unpredictable system impact

General Findings

Observation

If attacks cause spurious alarms, the system will be turned off

Attacks have real potential for disruption, though specific disruption is hard to predict

Participants generally fast to identify unusual behaviour

Effect

Attackers 'force' pilots away from systems by attacking them

Can have a wider, more unpredictable system impact

General Findings

Observation	Effect
If attacks cause spurious alarms, the system will be turned off	Attackers 'force' pilots away from systems by attacking them
Attacks have real potential for disruption, though specific disruption is hard to predict	Can have a wider, more unpredictable system impact
Participants generally fast to identify unusual behaviour	Indicates that existing procedure provides a sound base

General Findings

Observation | Effect

Observation	Effect
If attacks cause spurious alarms, the system will be turned off	Attackers 'force' pilots away from systems by attacking them
Attacks have real potential for disruption, though specific disruption is hard to predict	Can have a wider, more unpredictable system impact
Participants generally fast to identify unusual behaviour	Indicates that existing procedure provides a sound base
Attack success partly depends on wider system effects	

General Findings

Observation	Effect
If attacks cause spurious alarms, the system will be turned off	Attackers ‘force’ pilots away from systems by attacking them
Attacks have real potential for disruption, though specific disruption is hard to predict	Can have a wider, more unpredictable system impact
Participants generally fast to identify unusual behaviour	Indicates that existing procedure provides a sound base
Attack success partly depends on wider system effects	Traffic, weather, ATC load, pilot tiredness

Lessons Learned

Lessons Learned

1. ## Diagnosis is key

   Due to grey areas in procedure existing around the attacks, a lot of time was spent diagnosing the closest possible failure

Lessons Learned

1. **Diagnosis is key**

   Due to grey areas in procedure existing around the attacks, a lot of time was spent diagnosing the closest possible failure

2. **Value of simulation**

   Allows unexpected situations to emerge, scenarios to unfold fully and highlights factors which might not have been considered in analysis

Lessons Learned

1. ## Diagnosis is key

   Due to grey areas in procedure existing around the attacks, a lot of time was spent diagnosing the closest possible failure

2. ## Value of simulation

   Allows unexpected situations to emerge, scenarios to unfold fully and highlights factors which might not have been considered in analysis

3. ## Real usage matters

   Understanding how and why humans in the loop of safety critical systems act like they do is important in security analysis

Summary

- Attacks cause disruption, even when pilots can mitigate part of the effect of the attack
- Responses take a variety of forms, leading to attacks causing unpredictability
- In many cases, attacks push pilots to disable safety-related systems
- Existing procedure provides an ideal starting point for new steps to handle attacks

Questions

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

Matt Smith†, Martin Strohmeier$†, Jonathan Harman, Vincent Lenders$ and Ivan Martinovic†

†Department of Computer Science,
University of Oxford,
United Kingdom
Email: first.last@cs.ox.ac.uk
Twitter: @avsecoxford

$Cyber-Defence Campus,
armasuisse Science + Technology,
Switzerland
Email: first.last@armasuisse.ch
Twitter: @cydcampus

References

- [1] - On Perception and Reality in Wireless Air Traffic Communication Security. Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders and Ivan Martinovic. In IEEE Transactions on Intelligent Transportation Systems. Vol. 18. No. 6. Pages 1338—1357. June, 2017.
- [2] –Wireless attacks on aircraft instrument landing systems. Sathaye, Harshad, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. In 28th {USENIX} Security Symposium ({USENIX} Security 19), pp. 357-372. 2019.
- [3] – Experimental analysis of attacks on next generation air traffic communication. Schäfer, Matthias, Vincent Lenders, and Ivan Martinovic. In International Conference on Applied Cryptography and Network Security, pp. 253-271. Springer, Berlin, Heidelberg, 2013.

  Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. Costin, Andrei, and Aurélien Francillon. Black Hat USA (2012): 1-12.
- [4] - Original uploader Tswgb. Edit by Abuk SABUK https://commons.wikimedia.org/wiki/File:PAPI_Jersey_Airport.JPG
- [5] - https://commons.wikimedia.org/wiki/File:Baltic_Aviation_Academy_Airbus_B737_Full_Flight_Simulator_(FFS).jpg
- Slide 1 - Photo by NeONBRAND on Unsplash - https://unsplash.com/photos/c56y966zOXc
- Slide 19 - Photo by Eric Bruton on Unsplash