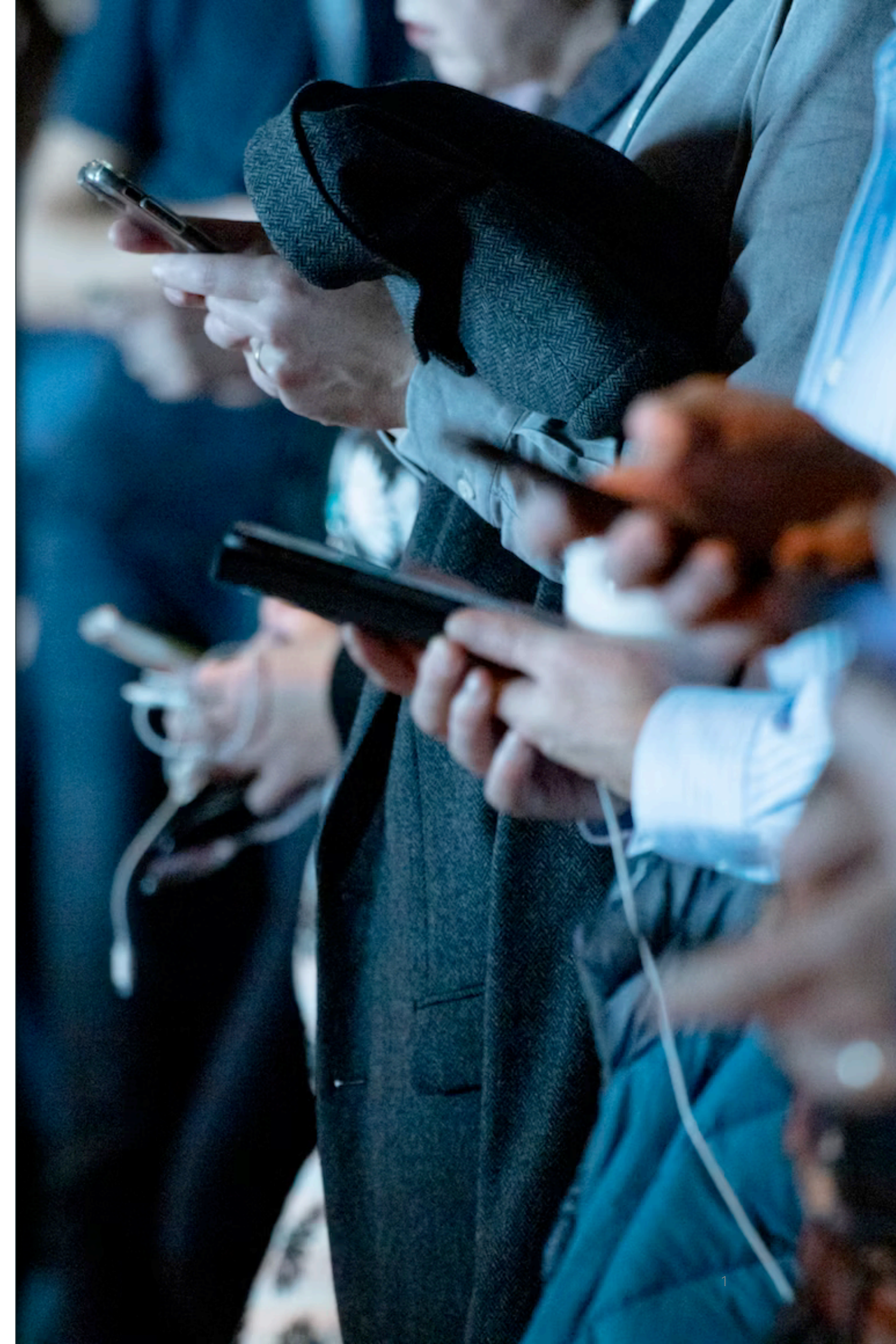
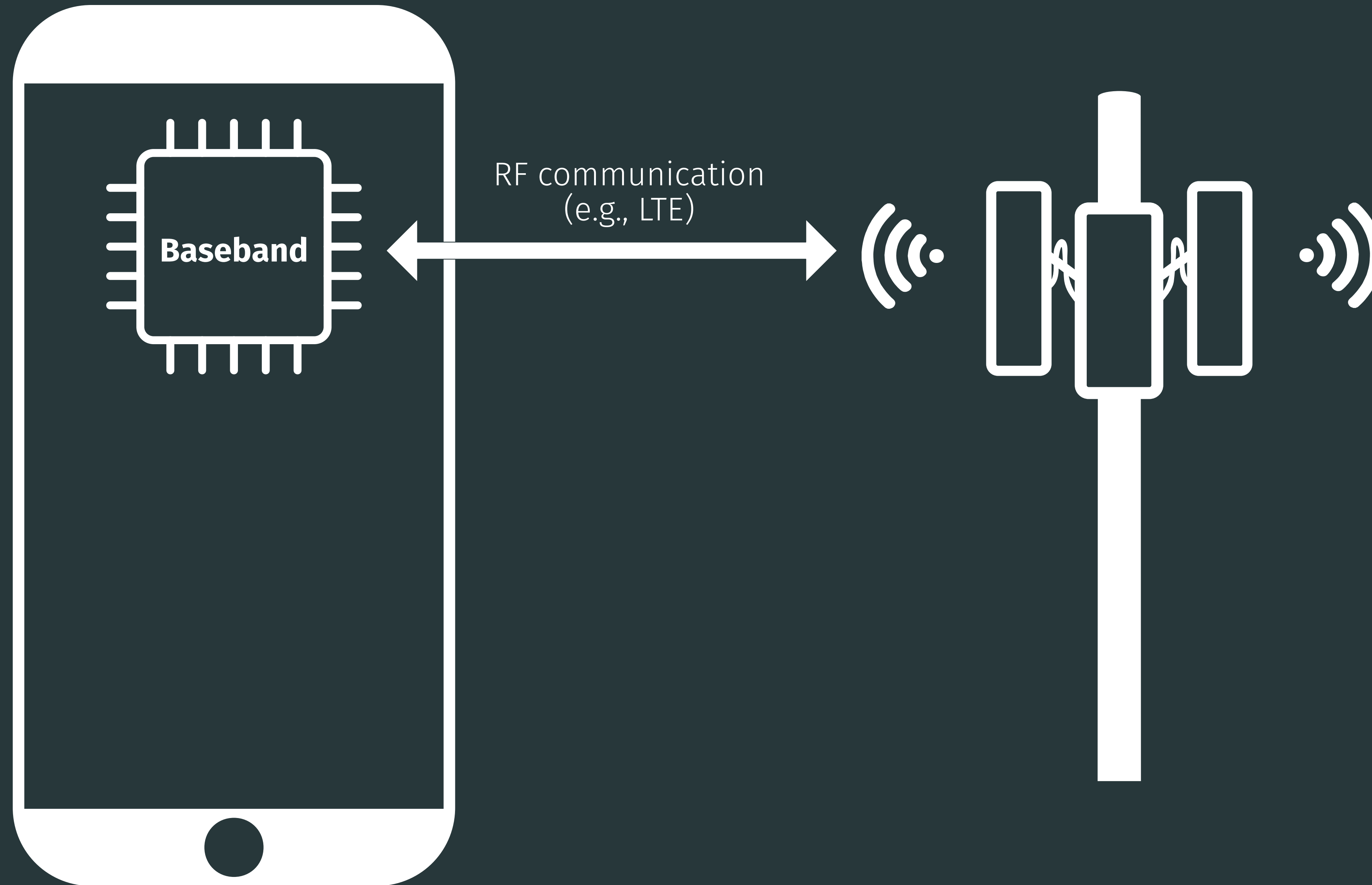


Instructions Unclear: Undefined Behaviour in Cellular Network Specifications

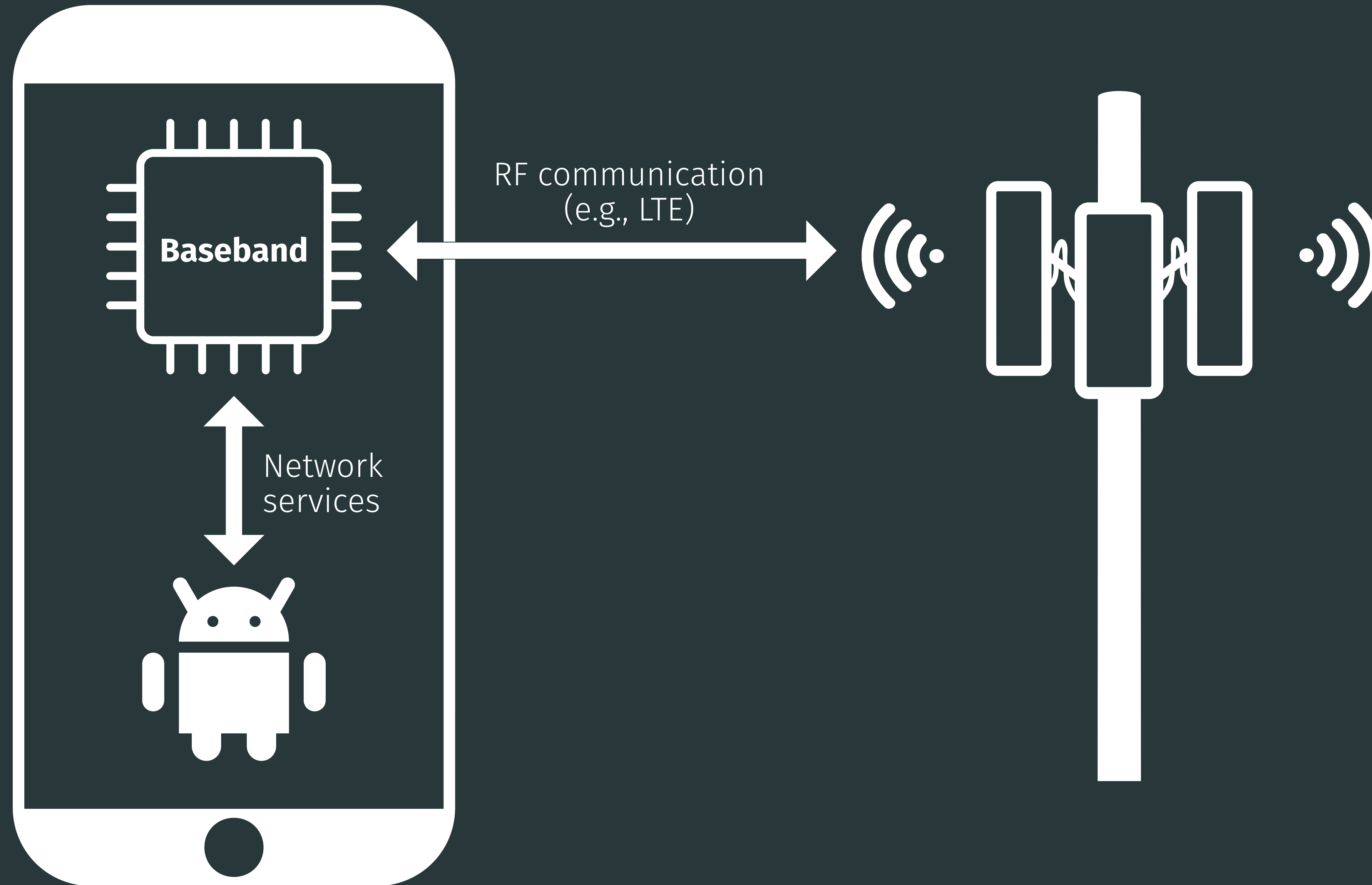
Daniel Klischies, Moritz Schloegel, Tobias Scharnowski
Mikhail Bogodukhov, David Rupprecht, Veelasha Moonsamy



Cellular baseband



Cellular baseband





WWLP Springfield

+ Follow

FLASH FLOOD WARNING issued across cell phones in Massachusetts

Story by Amy Phillips • Tuesday

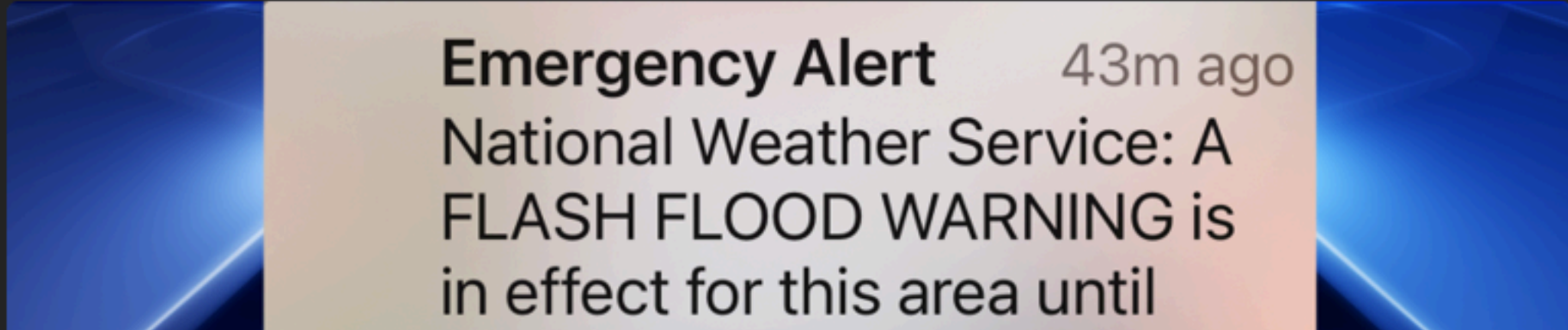
CHICOPEE, Mass. (WWLP) – The National Weather Service issued a Flash Flood Warning for parts of western Massachusetts Tuesday afternoon that may have caught you by surprise on your cell phone.

[Weather Alert: Possible strong thunderstorms Tuesday](#)

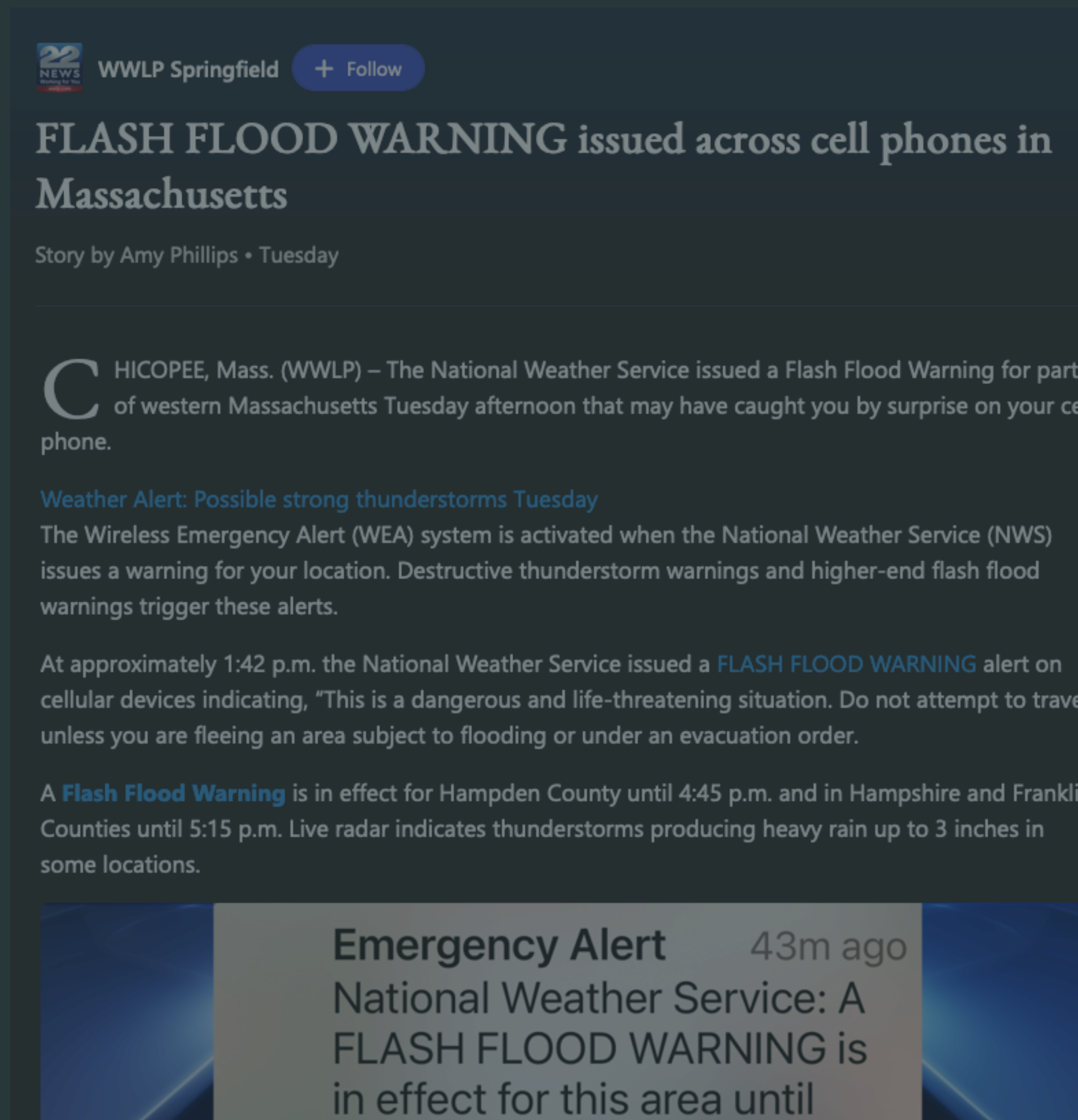
The Wireless Emergency Alert (WEA) system is activated when the National Weather Service (NWS) issues a warning for your location. Destructive thunderstorm warnings and higher-end flash flood warnings trigger these alerts.

At approximately 1:42 p.m. the National Weather Service issued a **FLASH FLOOD WARNING** alert on cellular devices indicating, "This is a dangerous and life-threatening situation. Do not attempt to travel unless you are fleeing an area subject to flooding or under an evacuation order.

A **Flash Flood Warning** is in effect for Hampden County until 4:45 p.m. and in Hampshire and Franklin Counties until 5:15 p.m. Live radar indicates thunderstorms producing heavy rain up to 3 inches in some locations.



Emergency Alert 43m ago
National Weather Service: A
FLASH FLOOD WARNING is
in effect for this area until



WWLP Springfield + Follow

FLASH FLOOD WARNING issued across cell phones in Massachusetts

Story by Amy Phillips • Tuesday

CHICOPEE, Mass. (WWLP) – The National Weather Service issued a Flash Flood Warning for parts of western Massachusetts Tuesday afternoon that may have caught you by surprise on your cell phone.

Weather Alert: Possible strong thunderstorms Tuesday

The Wireless Emergency Alert (WEA) system is activated when the National Weather Service (NWS) issues a warning for your location. Destructive thunderstorm warnings and higher-end flash flood warnings trigger these alerts.

At approximately 1:42 p.m. the National Weather Service issued a **FLASH FLOOD WARNING** alert on cellular devices indicating, "This is a dangerous and life-threatening situation. Do not attempt to travel unless you are fleeing an area subject to flooding or under an evacuation order."

A **Flash Flood Warning** is in effect for Hampden County until 4:45 p.m. and in Hampshire and Franklin Counties until 5:15 p.m. Live radar indicates thunderstorms producing heavy rain up to 3 inches in some locations.

Emergency Alert 43m ago
National Weather Service: A FLASH FLOOD WARNING is in effect for this area until



BBC Home News Sport Reel Worklife Travel Future

NEWS

Home | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science | Entertainment | More

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

Hawaii missile false alarm triggers shock, blame and apologies

14 January 2018

EMERGENCY ALERTS now

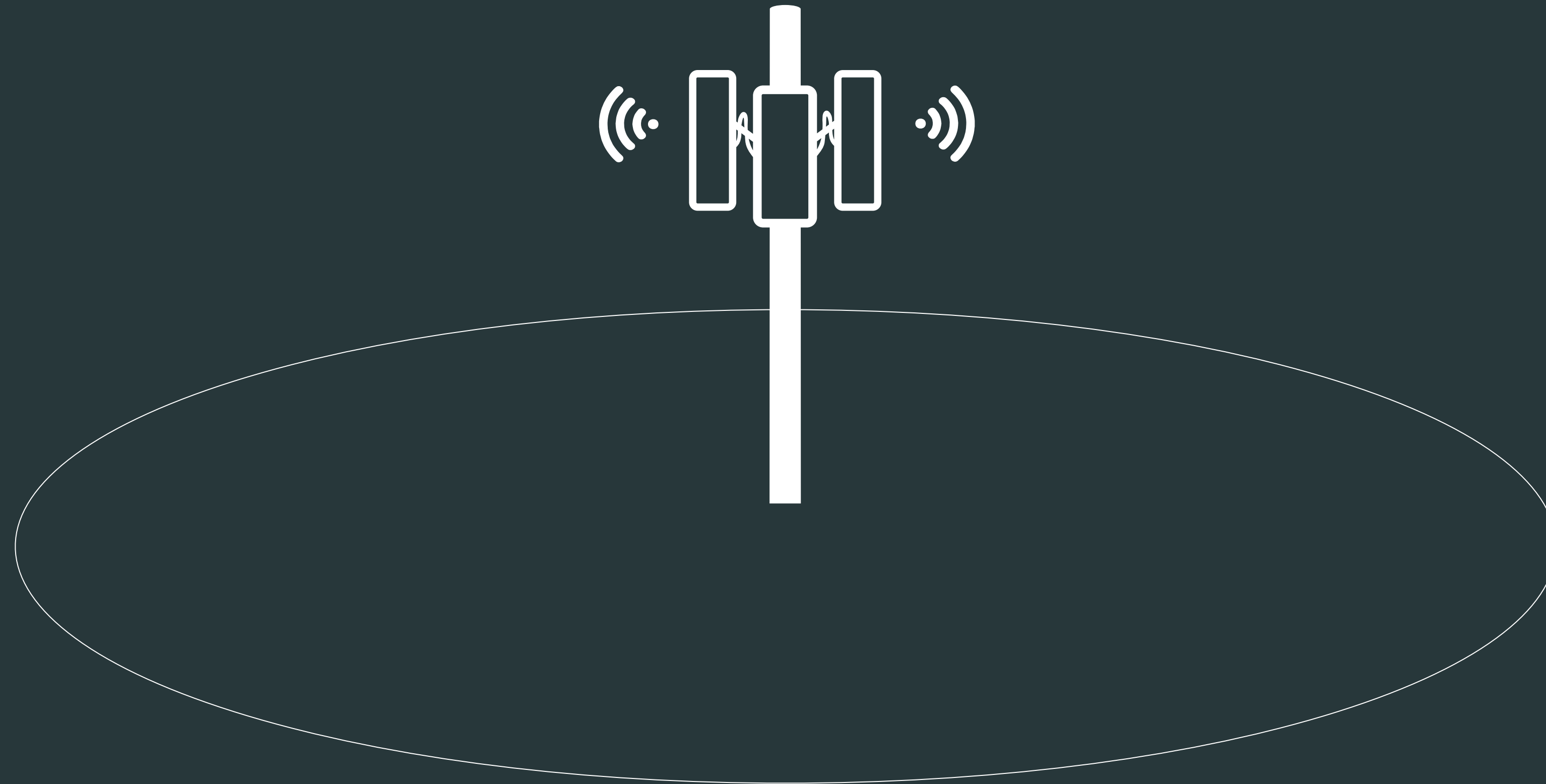
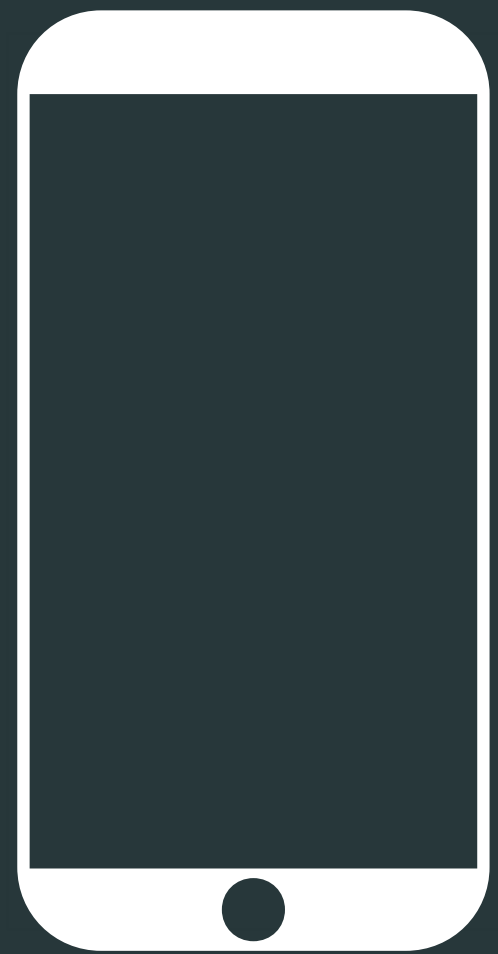
Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.
Slide for more

People were warned to take shelter

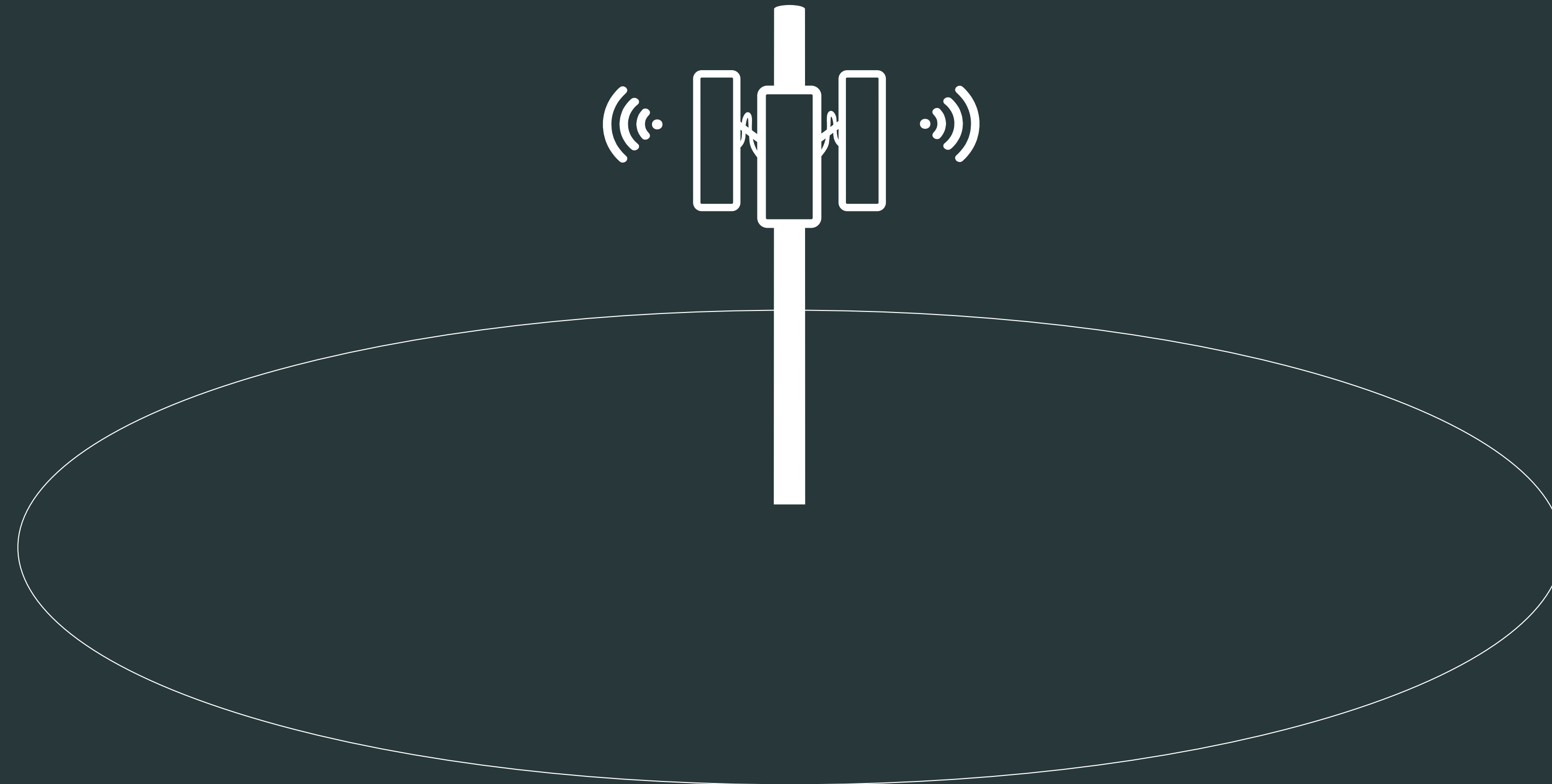
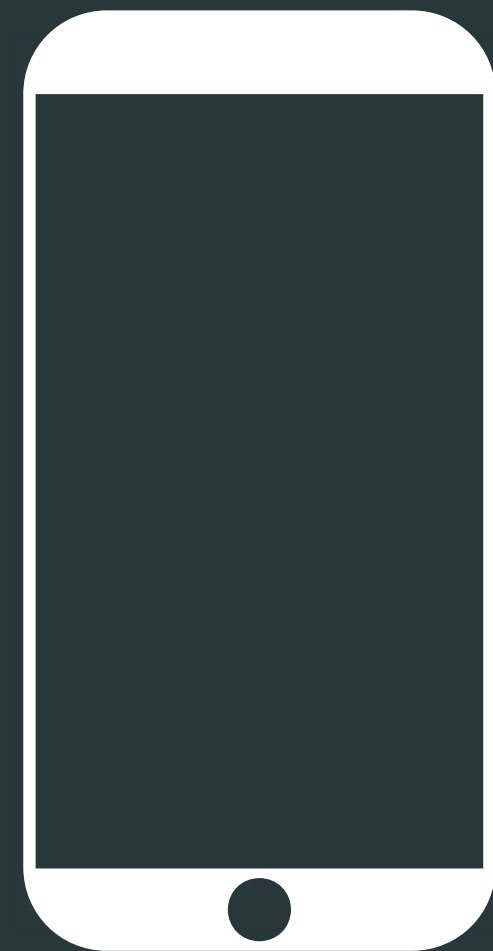
Residents and visitors in Hawaii have been recalling the shock of a false missile alarm, with many saying they thought they were going to die.

The alert of an incoming ballistic missile was sent wrongly on Saturday morning by an emergency system worker.

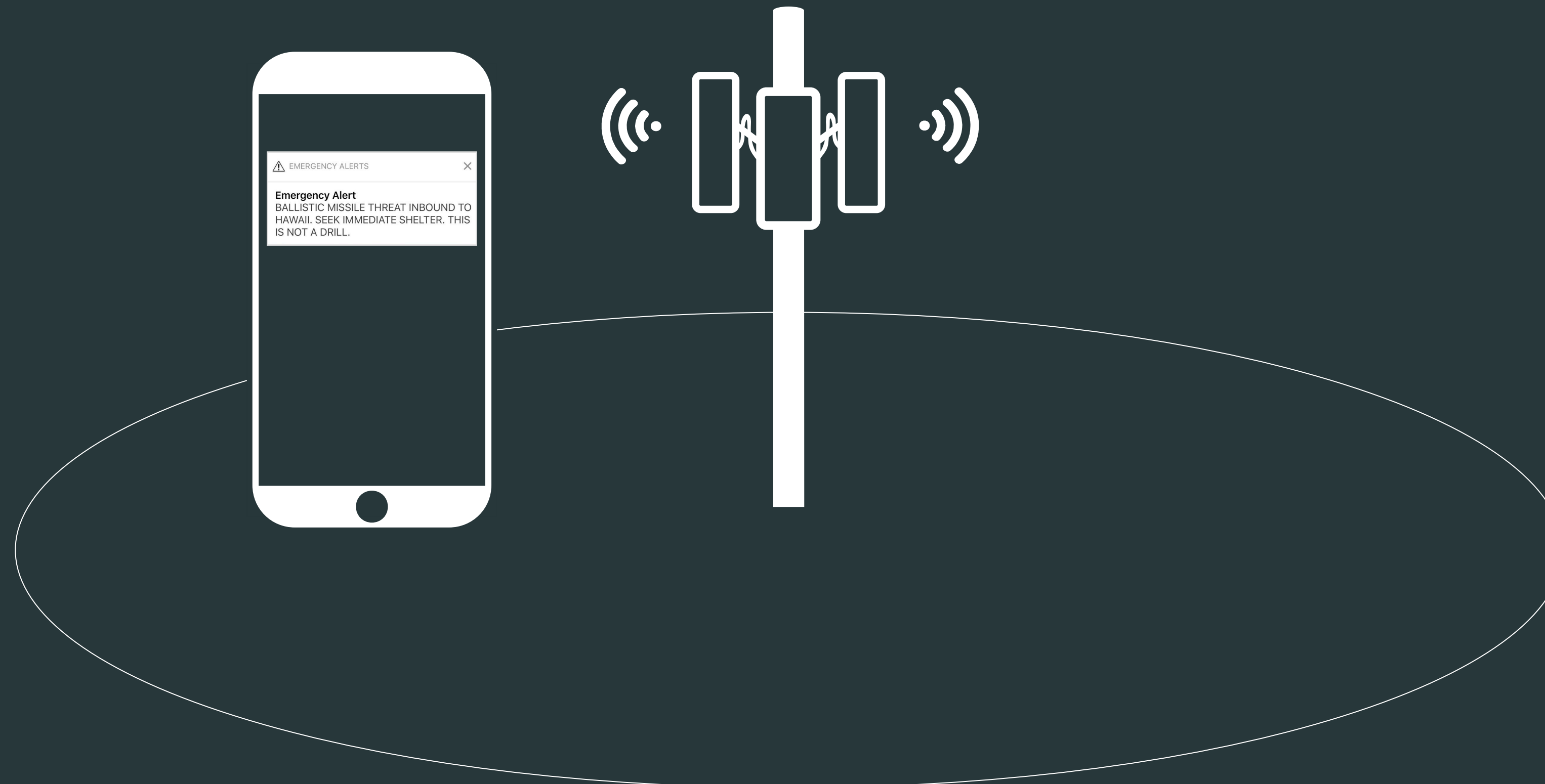
How your phone receives emergency alerts



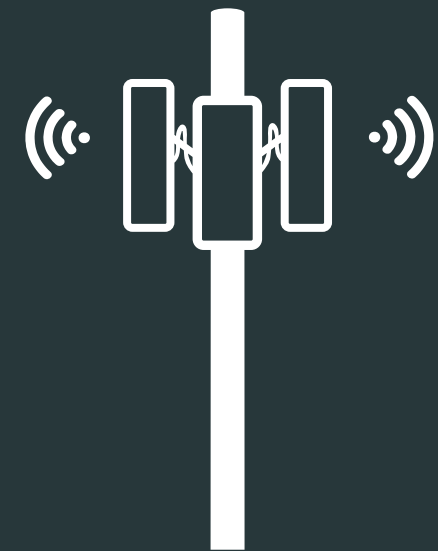
How your phone receives emergency alerts



How your phone receives emergency alerts



Behaviour of MediaTek's PWS implementation



Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND
Segment #: 2
lastSegment: y

Behaviour of MediaTek's PWS implementation



Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: INBOUND TO HAWAII
Segment #: 2 ←
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND
Segment #: 2
lastSegment: y

Behaviour of MediaTek's PWS implementation



Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes ←

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND
Segment #: 2
lastSegment: y

Behaviour of MediaTek's PWS implementation



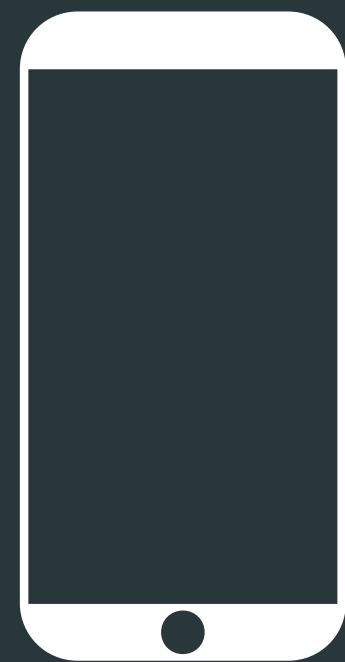
Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

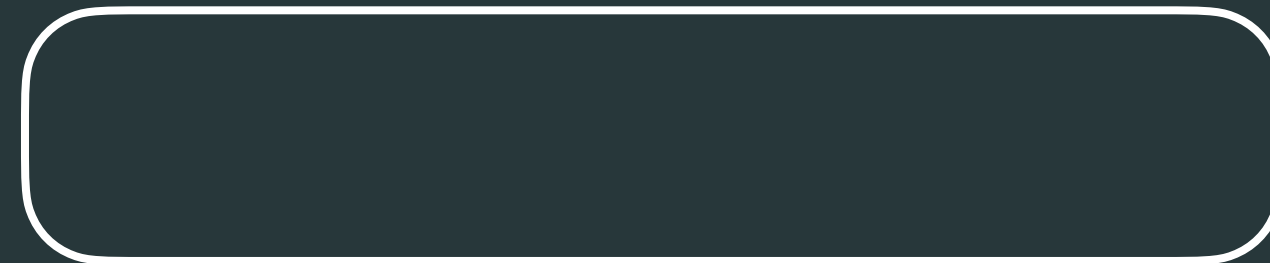
Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND
Segment #: 2
lastSegment: y



Baseband memory



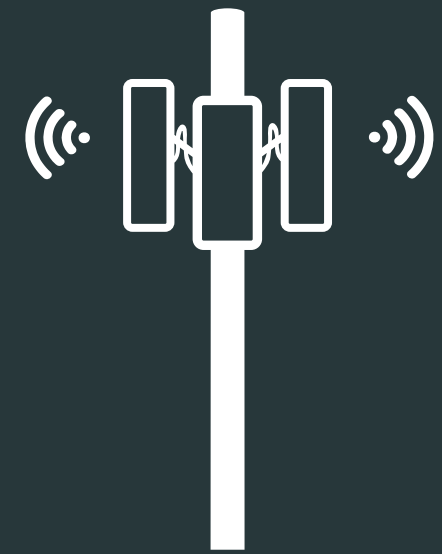
Received segments: 0



Target segments: ?



Behaviour of MediaTek's PWS implementation



Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

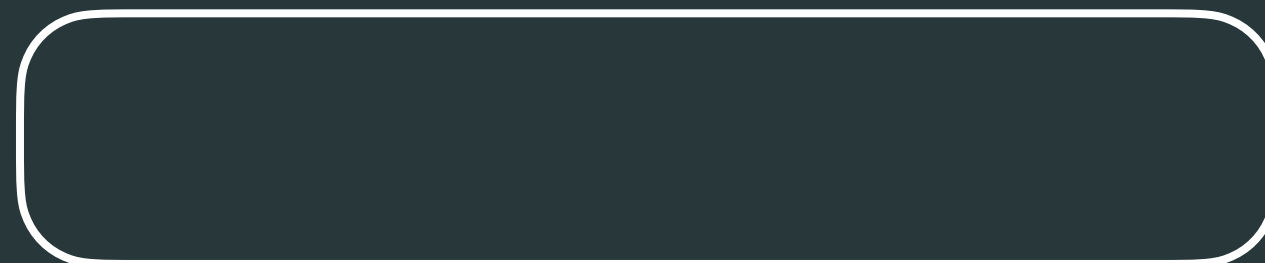
Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes



Baseband memory



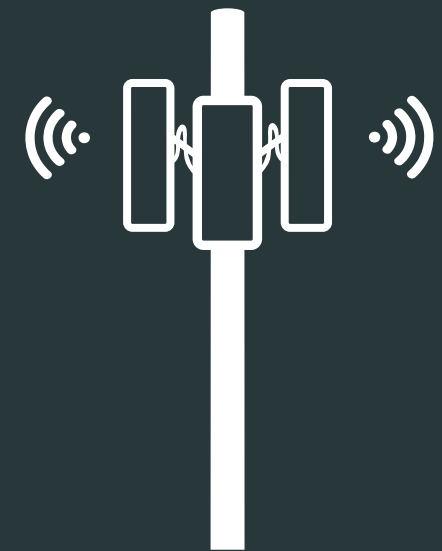
Received segments: 1



Target segments: ?



Behaviour of MediaTek's PWS implementation



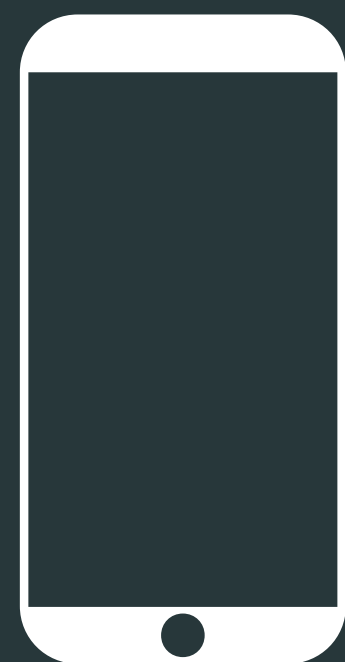
Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

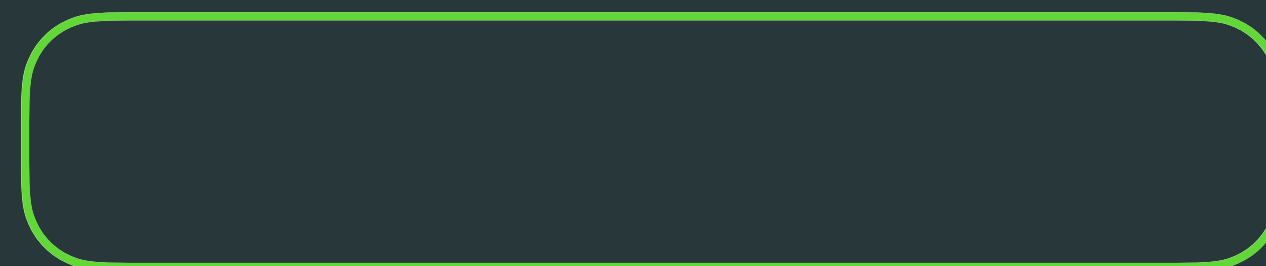
Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes



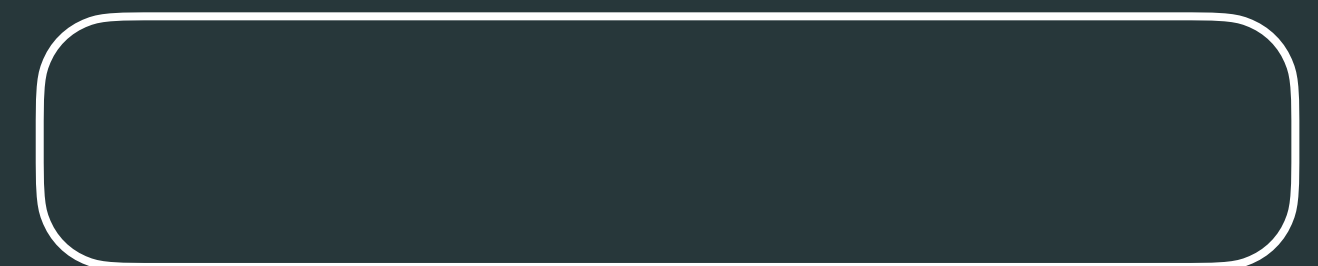
Baseband memory



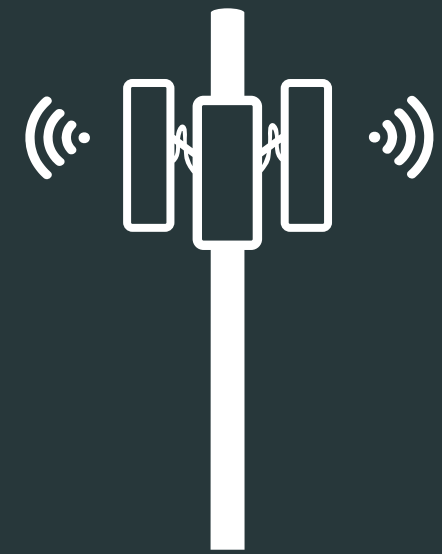
Received segments: 1



Target segments: 2



Behaviour of MediaTek's PWS implementation



Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE T
Segment #: 1
lastSegment: no

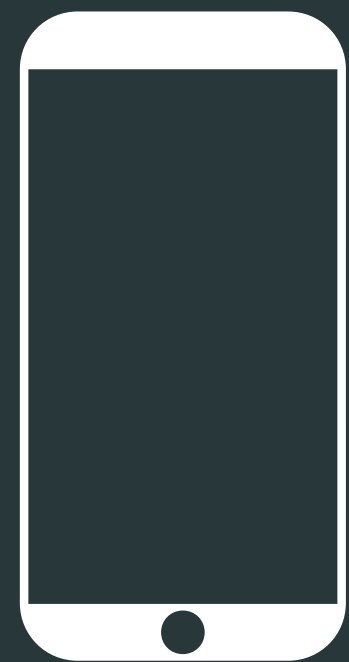
Baseband memory

BALLISTIC MISSILE THREAT

INBOUND TO HAWAII

Received segments: 2

Target segments: 2



Behaviour of MediaTek's PWS implementation



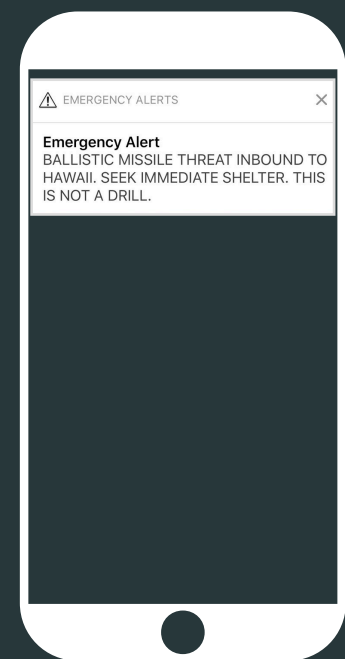
Text:

BALLISTIC MISSILE THREAT | INBOUND TO HAWAII

Text: BALLISTIC MISSILE THREAT
Segment #: 1
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE T
Segment #: 1
lastSegment: no



Baseband memory

BALLISTIC MISSILE THREAT INBOUND TO HAWAII

Received segments: 2

Target segments: 2

Undefined behaviour of MediaTek's PWS implementation

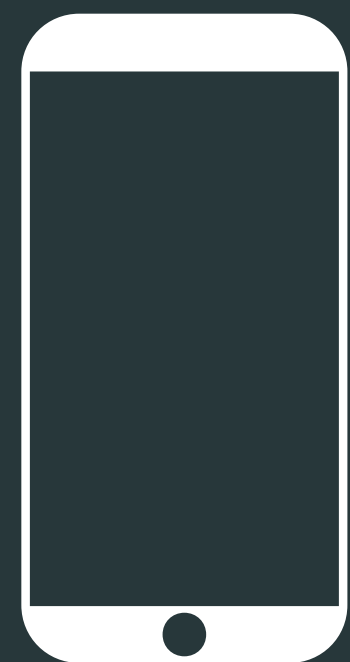


Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE THREAT
Segment #: 3
lastSegment: no



Text: INBOUND
Segment #: 2
lastSegment: y



Baseband memory



Received segments: 0



Target segments: ?



Undefined behaviour of MediaTek's PWS implementation

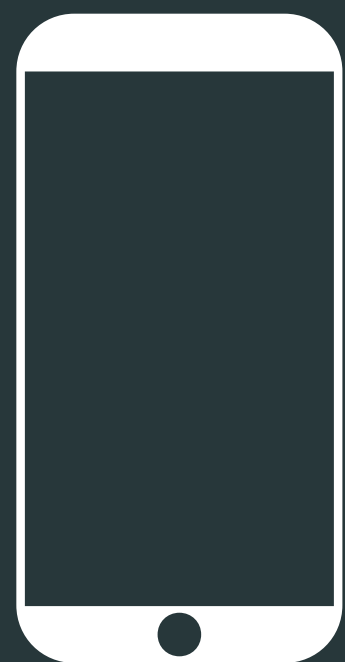


Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

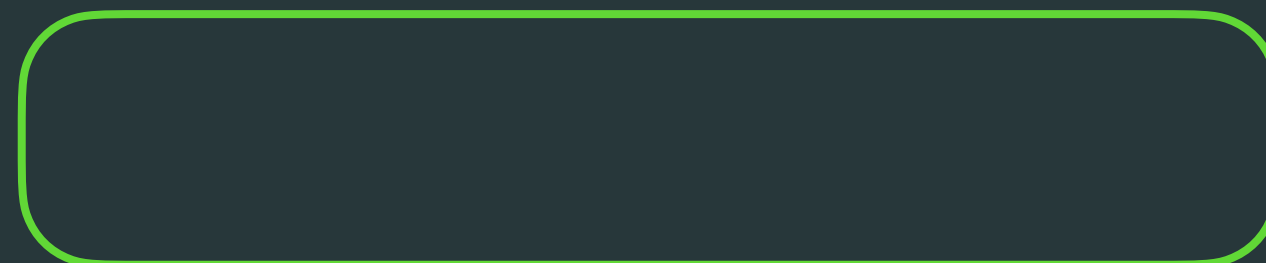
Text: BALLISTIC MISSILE THREAT
Segment #: 3
lastSegment: no



Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes



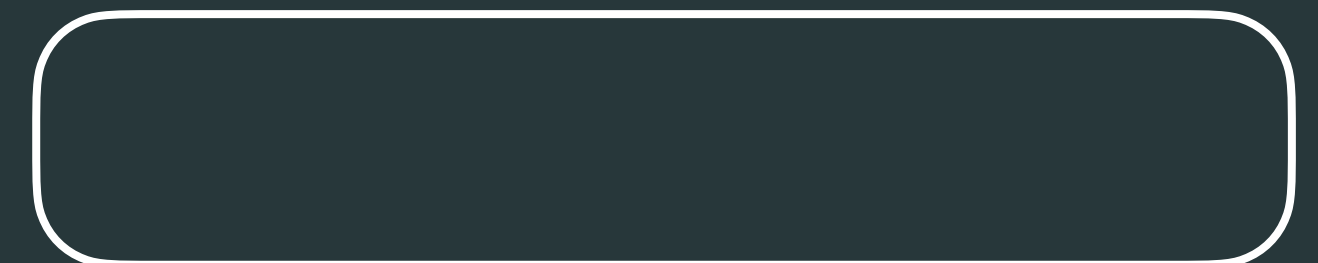
Baseband memory



Received segments: 1



Target segments: 2



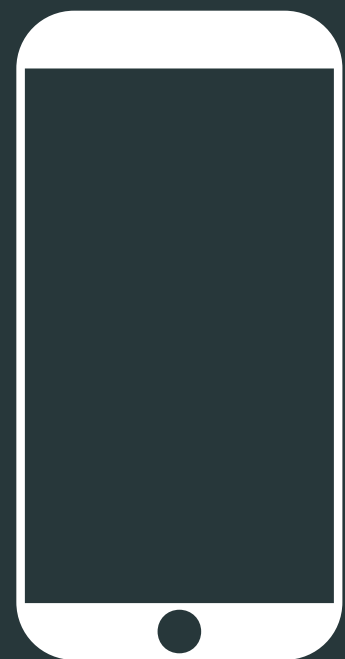
Undefined behaviour of MediaTek's PWS implementation



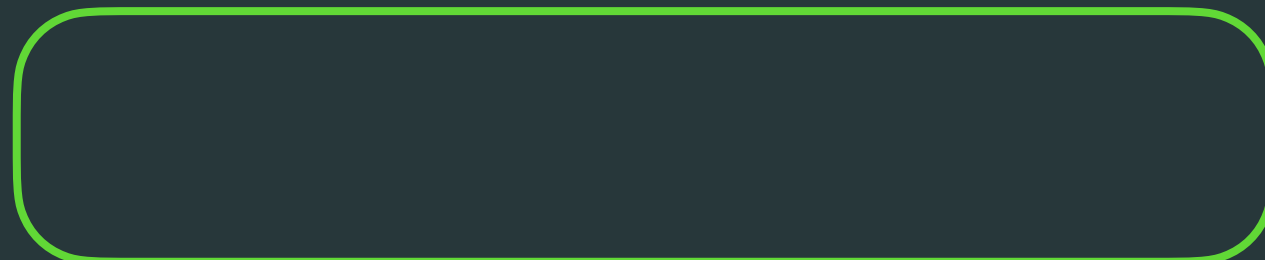
Text: BALLISTIC MISSILE THREAT
Segment #: 3
lastSegment: no

Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE T
Segment #: 3
lastSegment: no



Baseband memory



Received segments: 2



Target segments: 2



Undefined behaviour of MediaTek's PWS implementation

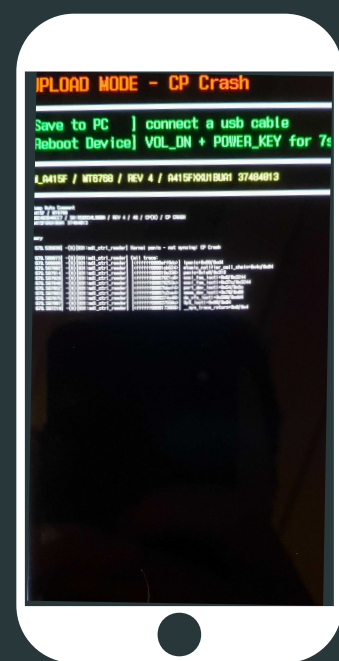


Text: BALLISTIC MISSILE THREAT
Segment #: 3
lastSegment: no



Text: INBOUND TO HAWAII
Segment #: 2
lastSegment: yes

Text: BALLISTIC MISSILE T
Segment #: 3
lastSegment: no



Baseband memory

<Uninitialized memory content> INBOUND TO HAWAII

BALLISTIC MISSILE THREAT

Received segments: 2

Target segments: 2

ETSI TS36.331, Section 5.2.2.19

5.2.2.19 Actions upon reception of *SystemInformationBlockType12*

Upon receiving *SystemInformationBlockType12*, the UE shall:

- 1> if the *SystemInformationBlockType12* contains a complete warning message:
 - 2> forward the received warning message, *messageIdentifier*, *serialNumber* and *dataCodingScheme* to upper layers;
 - 2> continue reception of *SystemInformationBlockType12*;
- 1> else:
 - 2> if the received values of *messageIdentifier* and *serialNumber* are the same (each value is the same) as a pair for which a warning message is currently being assembled:
 - 3> store the received *warningMessageSegment*;
 - 3> if all segments of a warning message have been received:
 - 4> assemble the warning message from the received *warningMessageSegment*;
 - 4> forward the received warning message, *messageIdentifier*, *serialNumber* and *dataCodingScheme* to upper layers;
 - 4> stop assembling a warning message for this *messageIdentifier* and *serialNumber* and delete all stored information held for it;
 - 3> continue reception of *SystemInformationBlockType12*;

How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19



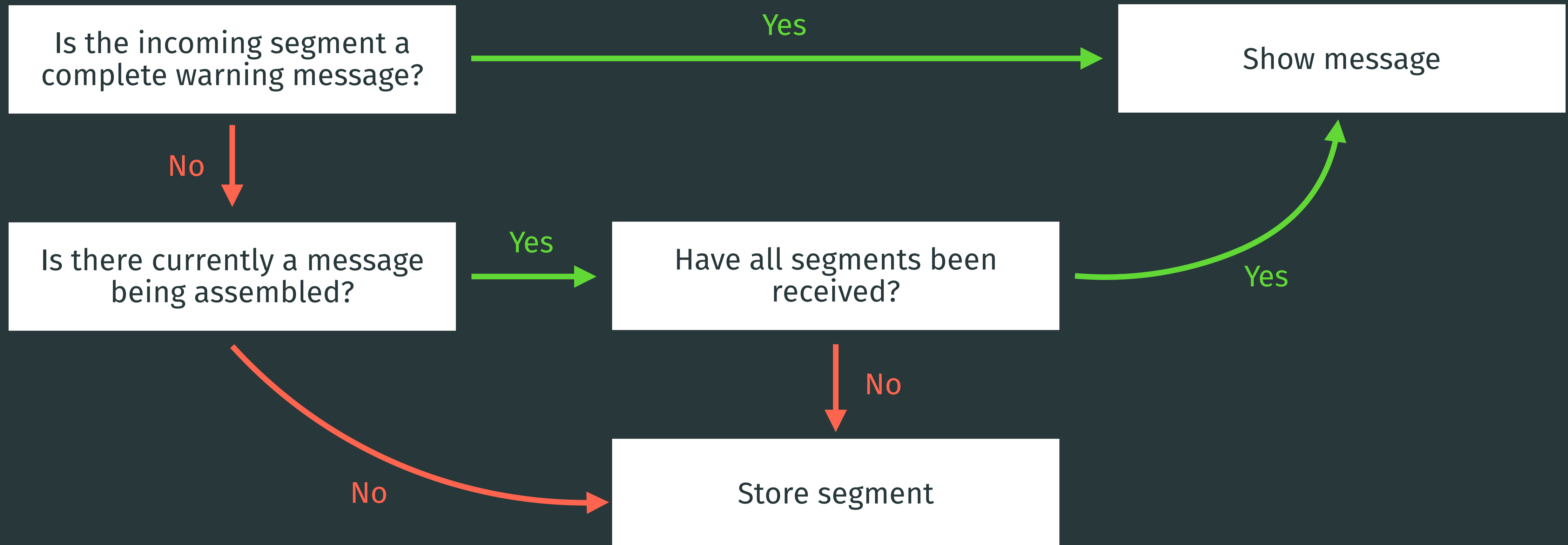
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19



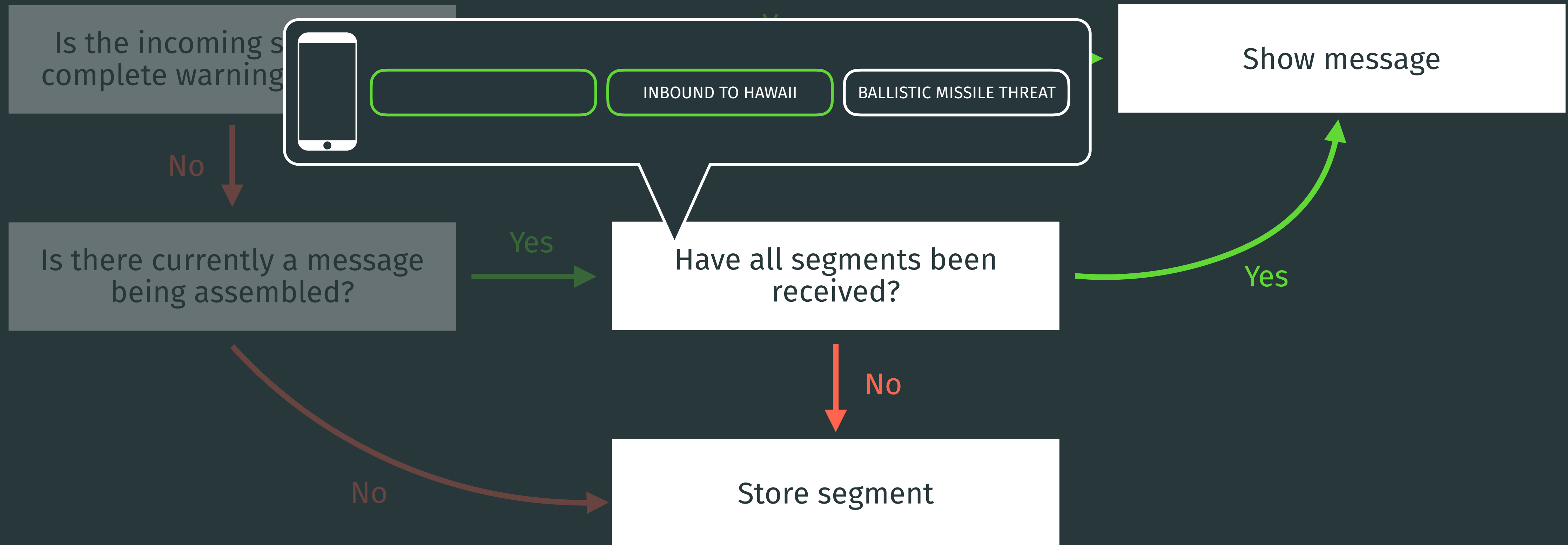
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19





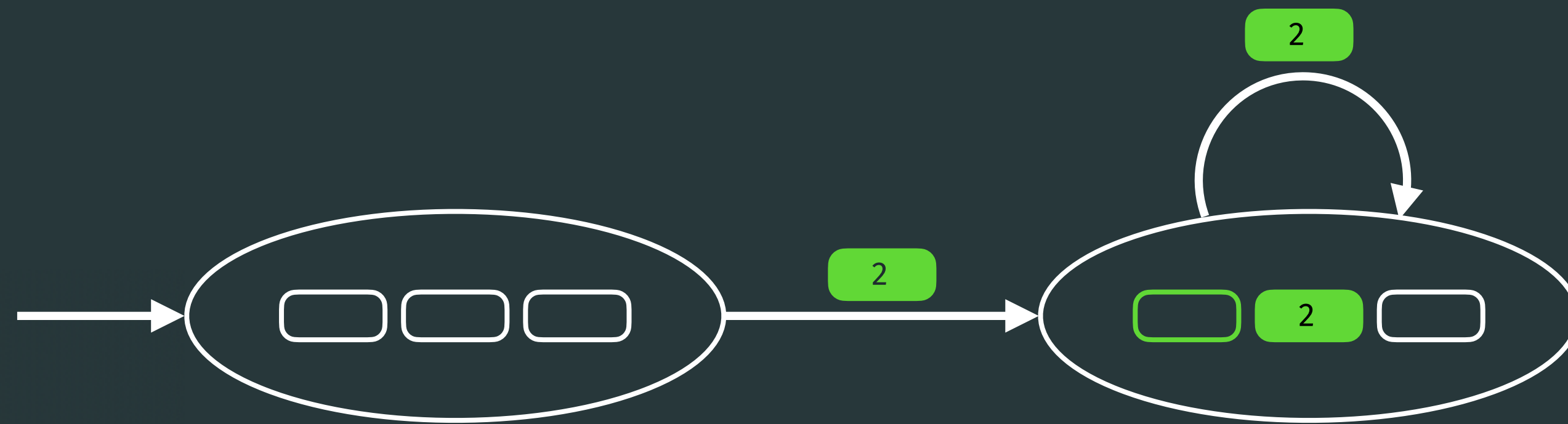
How did we discover this? Specifications.

ETSI TS36.331, Section 5.2.2.19





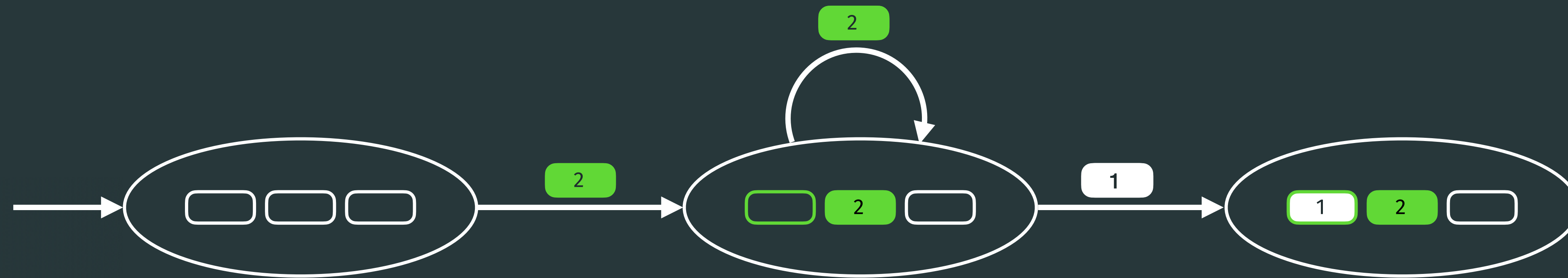
Specification as a state machine

-  Last segment
-  Not last segment





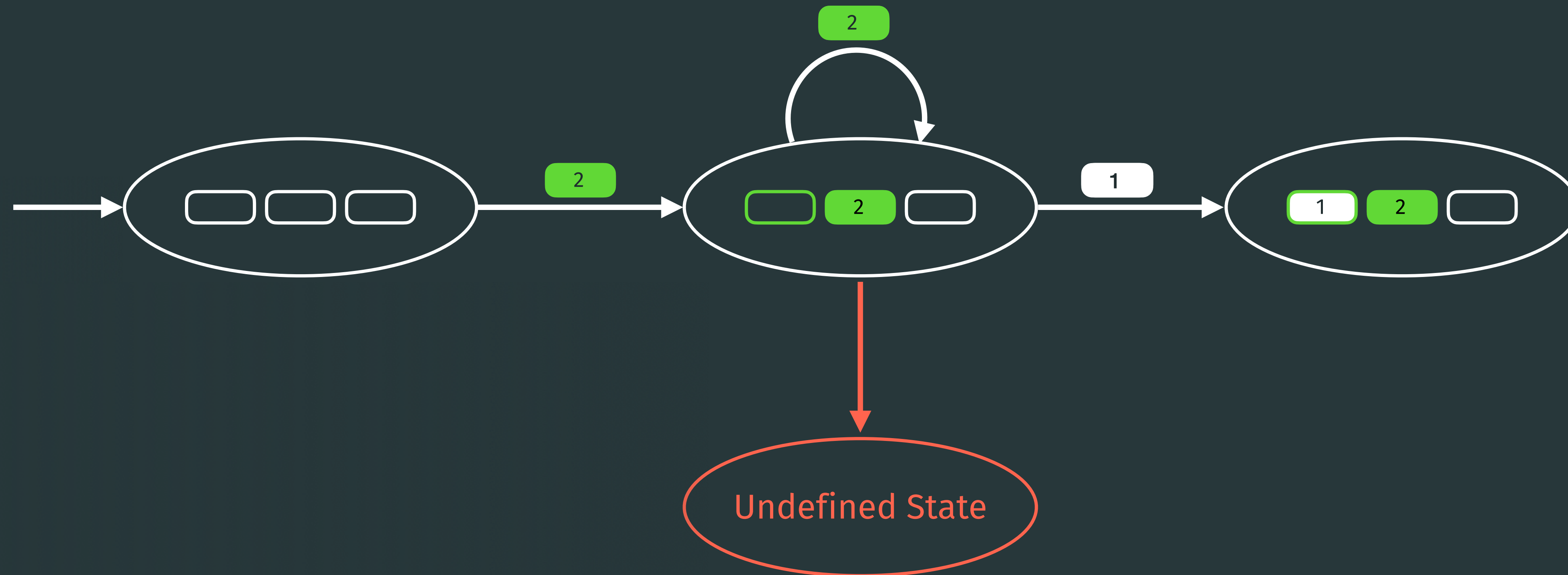
Specification as a state machine

-  Last segment
-  Not last segment





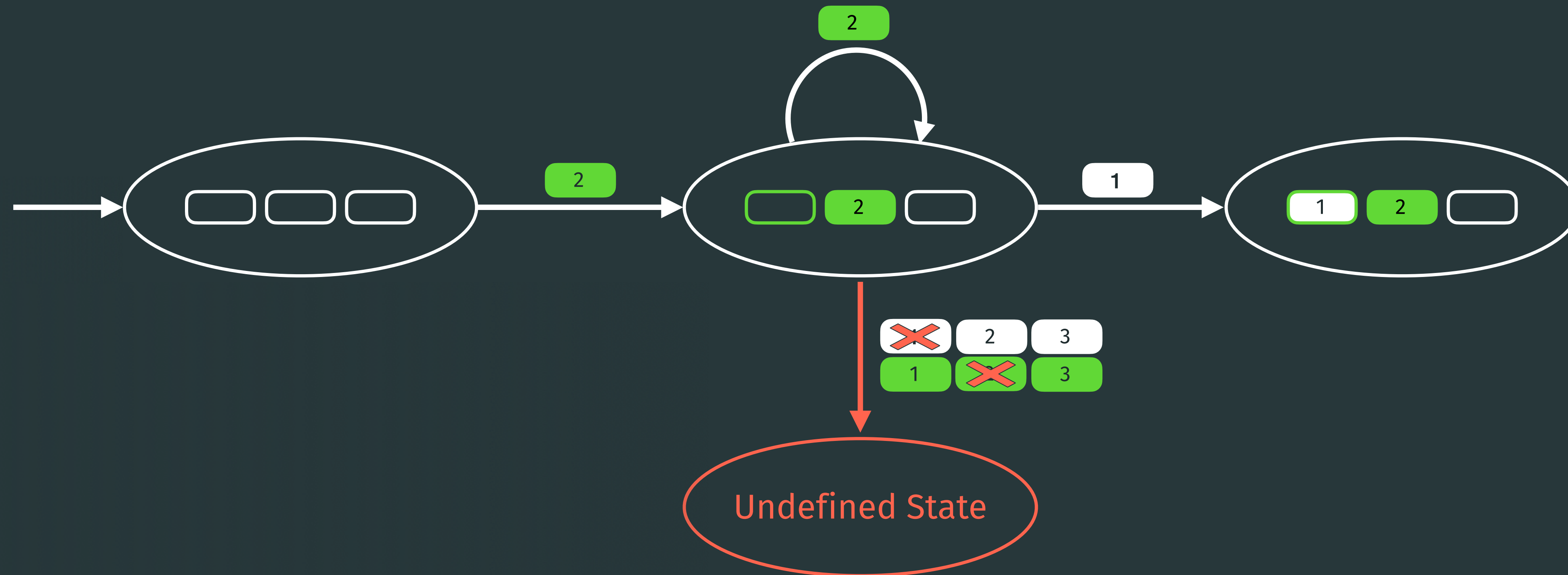
Specification as a state machine

-  Last segment
-  Not last segment



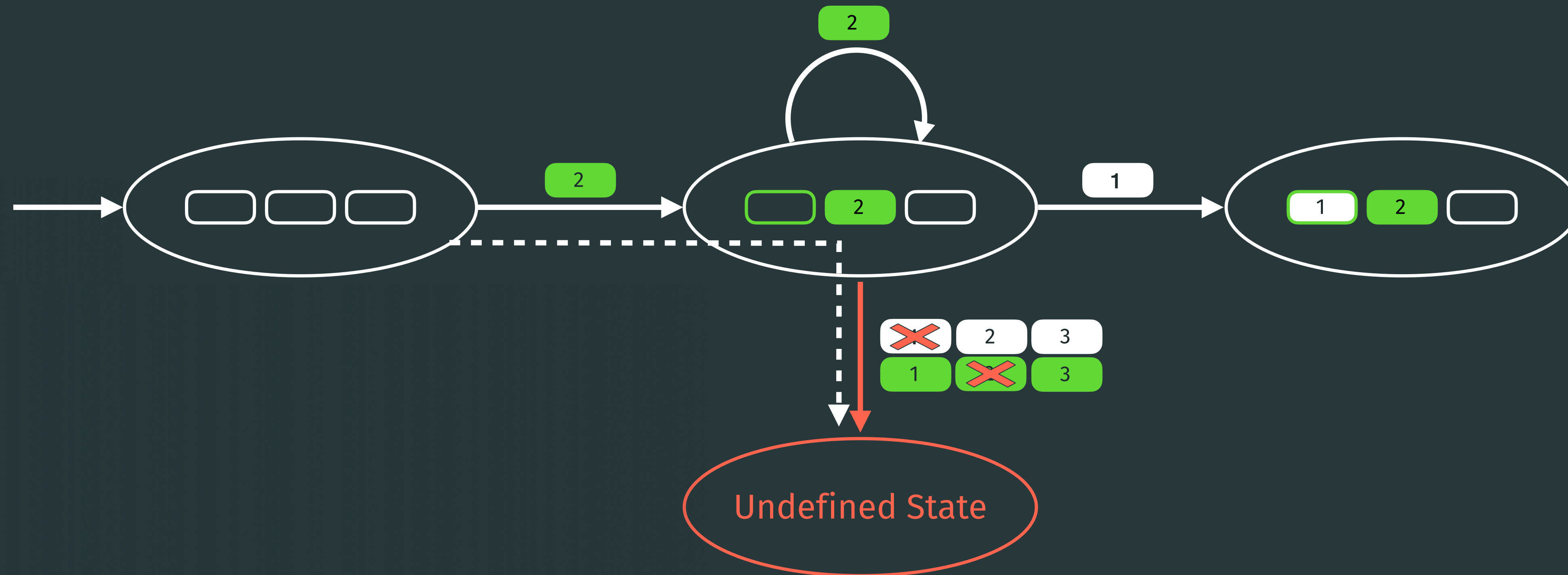
Specification as a state machine

-  Last segment
-  Not last segment





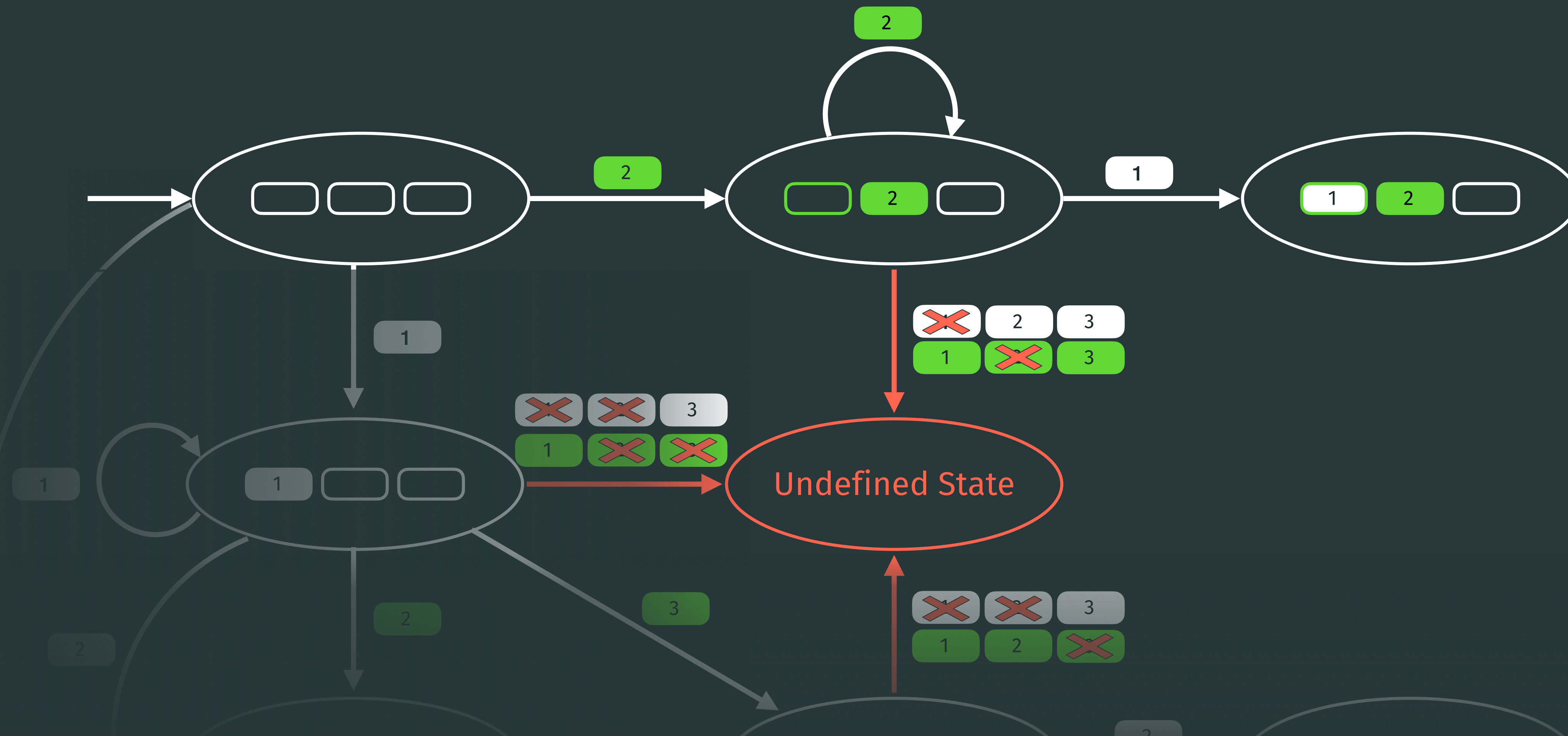
Specification as a state machine

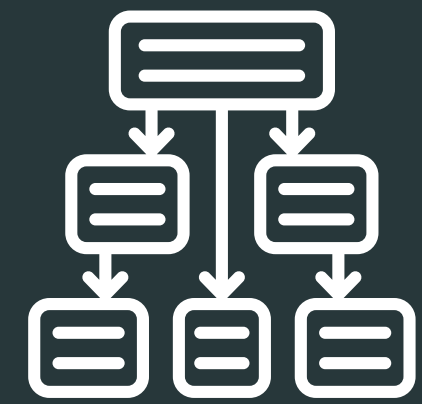
- Last segment
- Not last segment



Specification as a state machine

-  Last segment
-  Not last segment

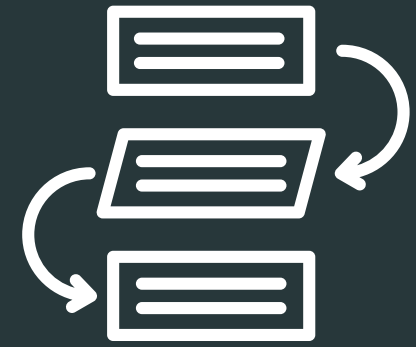




Dependencies within a network packet, like segment number and type



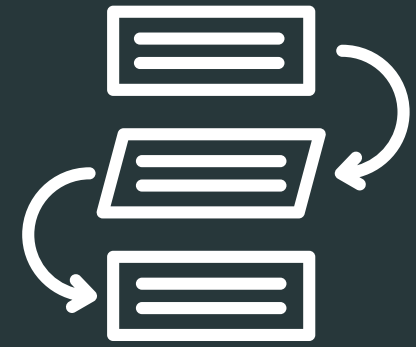
Dependencies within a network packet, like segment number and type



Packet **sequences** for state setup, fragmentation & reassembly



Dependencies within a network packet, like segment number and type



Packet **sequences** for state setup, fragmentation & reassembly



Timers for deduplication, timeouts & expiry

Our proposed approach: Using a model checker

Model defined behaviour

- Using mathematical notation → **Dependencies**
- And temporal logic → **Sequences & Timers**

} TLA+

Our proposed approach: Using a model checker

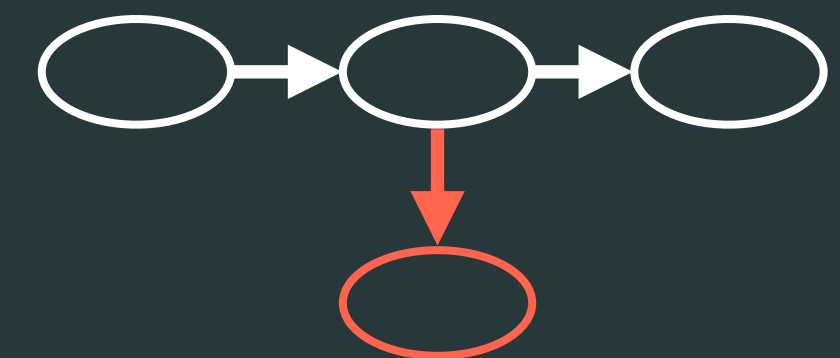
Model defined behaviour

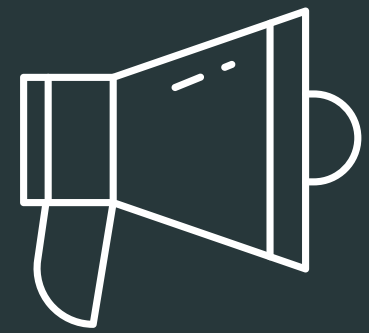
- Using mathematical notation → **Dependencies**
- And temporal logic → **Sequences & Timers**

} TLA+

Amend model to cover undefined behaviour

- Add an **undefined state**
- By negating the transitions for defined behaviour





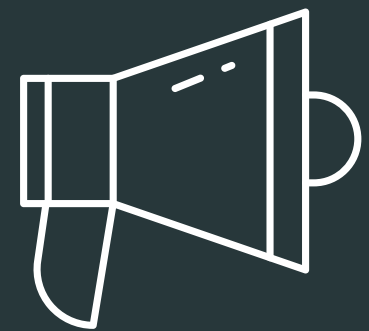
Public
Warning System



SMS



Radio
Resource Control



Public Warning System

14 million states

8 undefined
behaviours



SMS

8.5 million states

22 undefined
behaviours

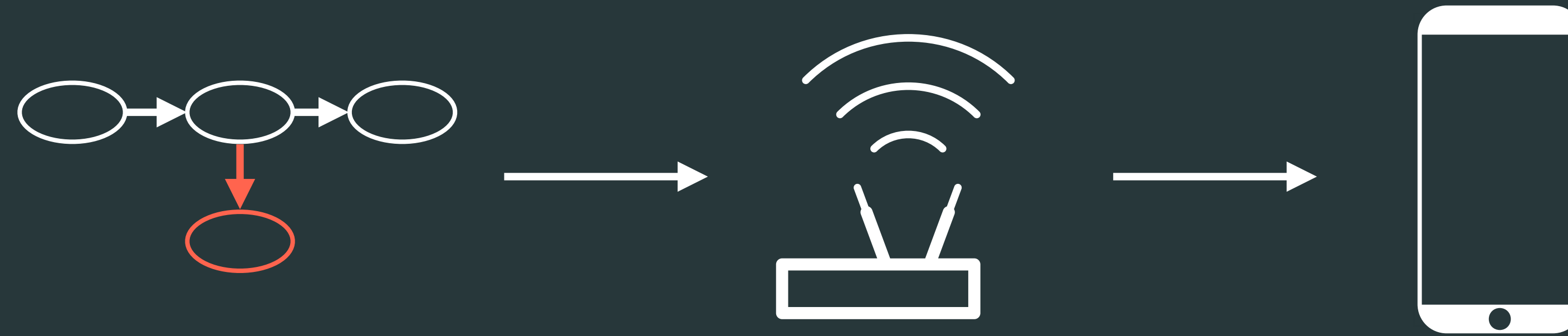


Radio Resource Control

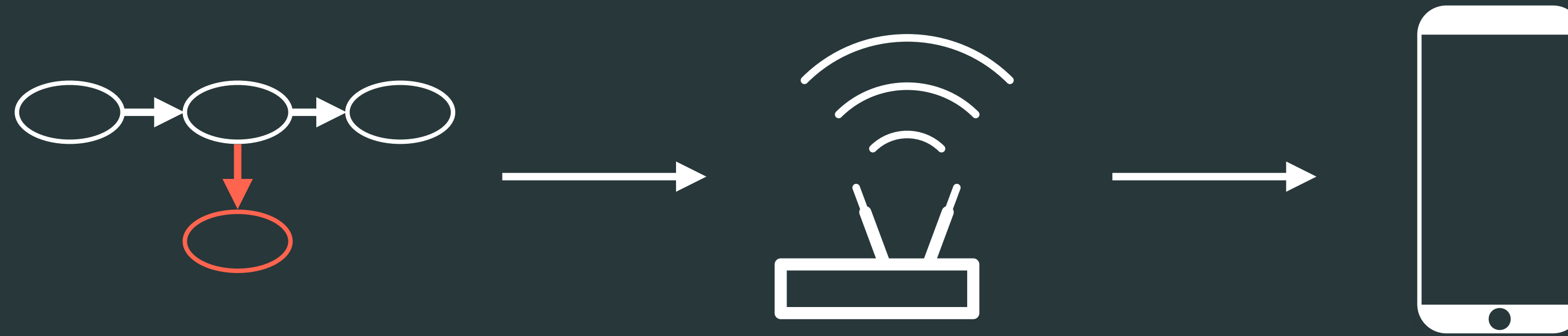
955 states

28 undefined
behaviours

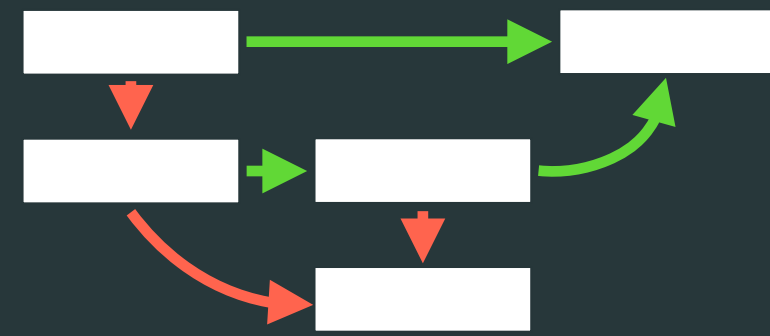
Over-the-air evaluation



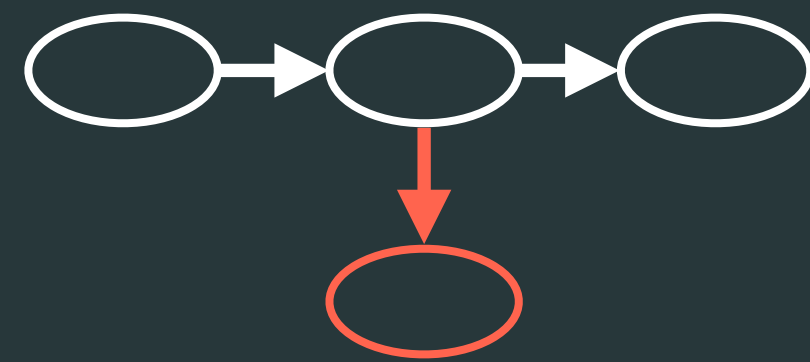
Over-the-air evaluation



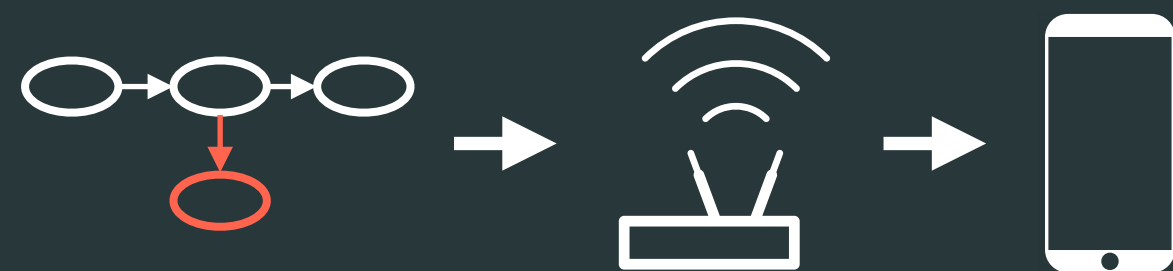
5 exploitable undefined behaviours
→ 3 CVEs



Cellular specifications contain undefined behaviour



Undefined behaviour can be discovered from a model of defined behaviour



Undefined behaviour promotes insecure implementations



Preprint
and artifacts