Hacking Driverless Vehicles

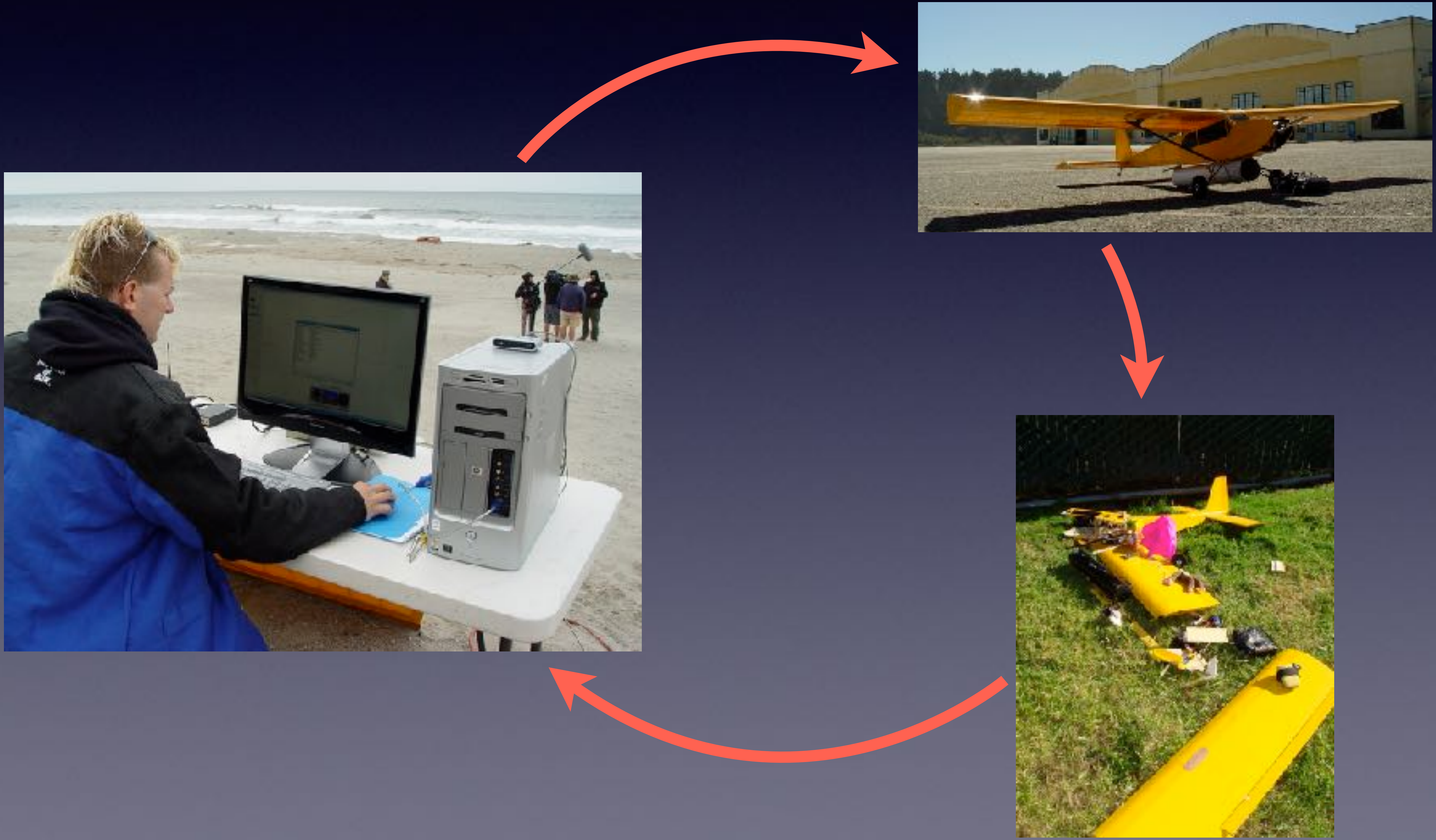
HACKING FOR B33R

BRUCON

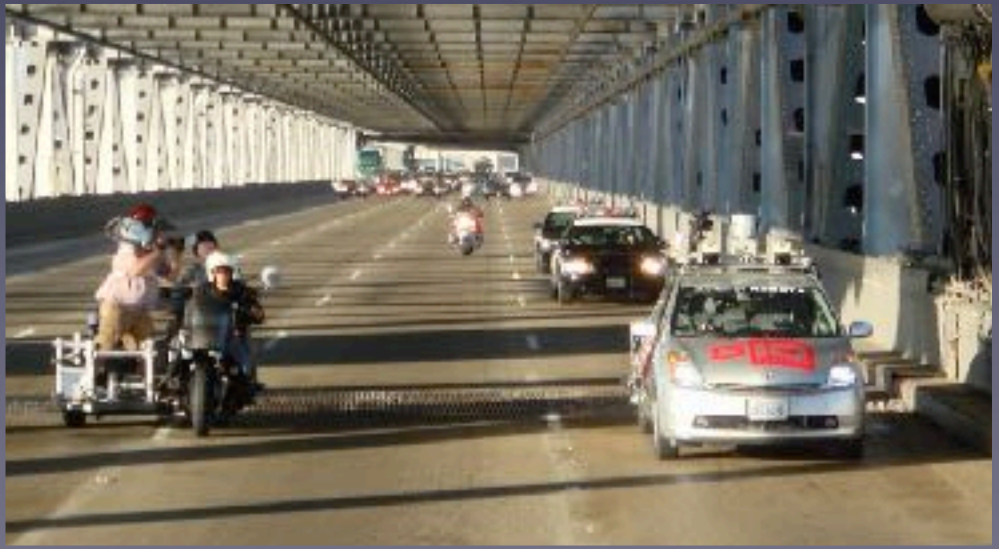
WWW.BRUCON.ORG

Zoz

PROTOTYPE
THIS



PROTOTYPE THIS



robonation
ROBOTICS COMMUNITY

Intelligent Ground Vehicle Competition

Student Unmanned Aerial Systems

RoboBoat

RoboSub

International Aerial Robotics Competition

Maritime RobotX

AUVSI foundation
ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS INTERNATIONAL

The Revolution Is Coming

- Advantages:
  - Energy efficiency
  - Time efficiency
  - New applications

The Revolution Is Coming

Europe

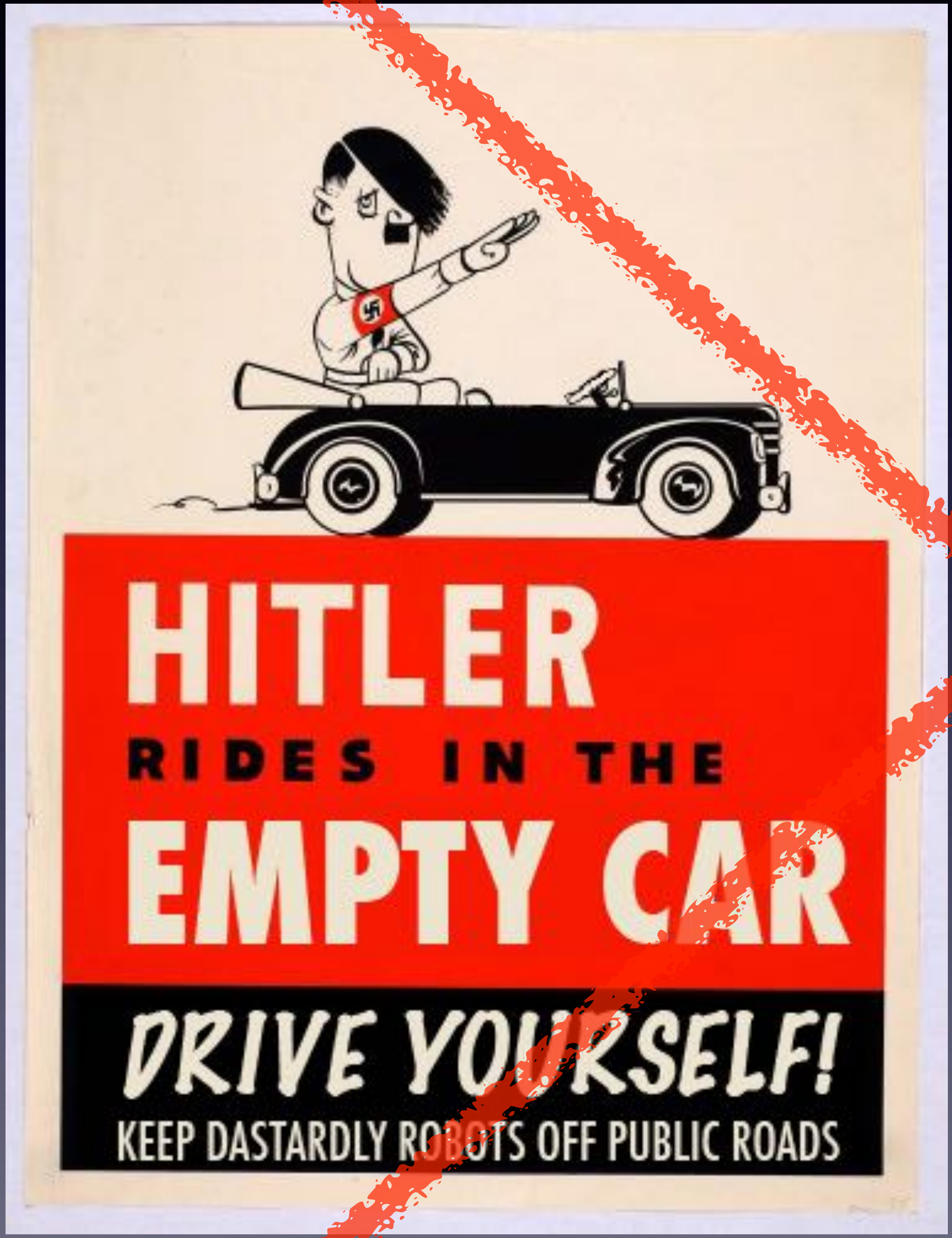
- UK: On-road testing in up to 3 cities starting 2015
  - £10 million research fund
- Sweden: 100 driverless Volvos in Gothenburg in 2017
- Undoubtedly more to come...

Europe

connected
automated
driving.eu

- UK: Nissan testing autonomous LEAFs in London since 2017
    - Jaguar Land Rover testing on public roads
    - Government promises £200 million research fund
- Sweden: Gothenburg driverless Volvo trials start Dec 2017 through 2018
    - Autonomous bus in northern Stockholm approved 2018
- Germany: BMW testing 40 vehicles in Munich
    - Promises to sell autonomous electric vehicle for autobahn in 2021
    - Autonomous bus trials in 2018 at Berlin hospital and Bad Birnach, Bavaria
- France: automated shuttles in Paris from 2017
    - Legislation to allow open road testing
- EU project AUTOPILOT: 2017-2019, 6 cities, €25,000,000
- Belgium: First self-driving delivery van test 2018, Mechelen, max. speed 8 km/h

~~FUD~~

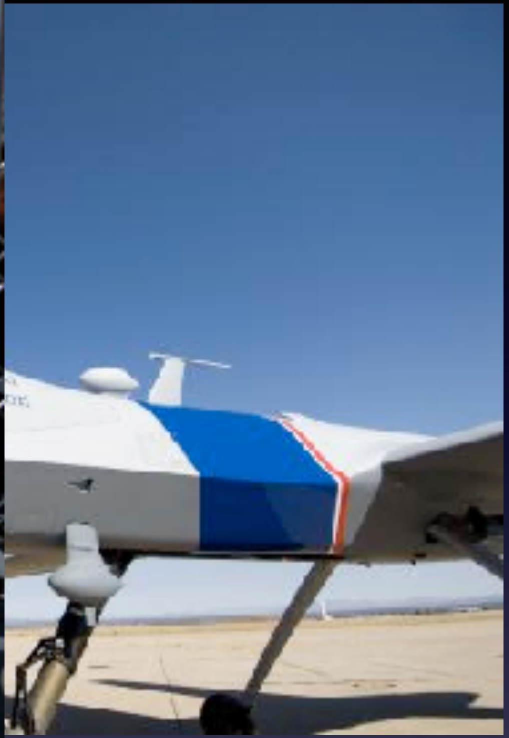

HITLER
RIDES IN THE
EMPTY CAR
DRIVE YOURSELF!
KEEP DASTARDLY ROBOTS OFF PUBLIC ROADS

When the car drives itself
you ride with Hitler !
Keep
your hands on the
WHEEL!

Autonomous/Unmanned Systems

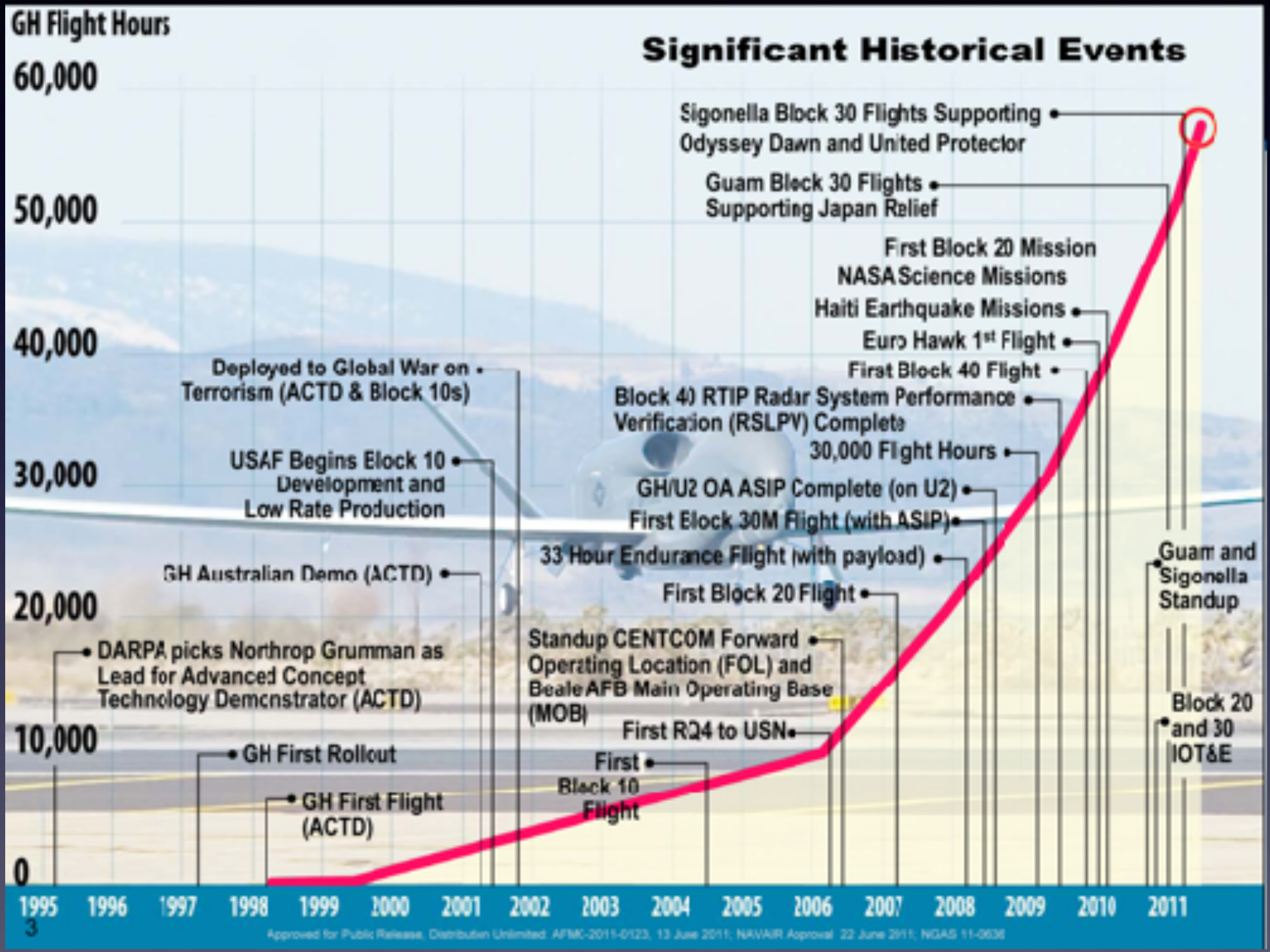
Autonomous/Unmanned Systems

Autonomous/Unmanned Systems



- No human driver/pilot on-board
- May have off-board controller/supervisor
- May have on-board safety pilot/passengers
- Military early adopters

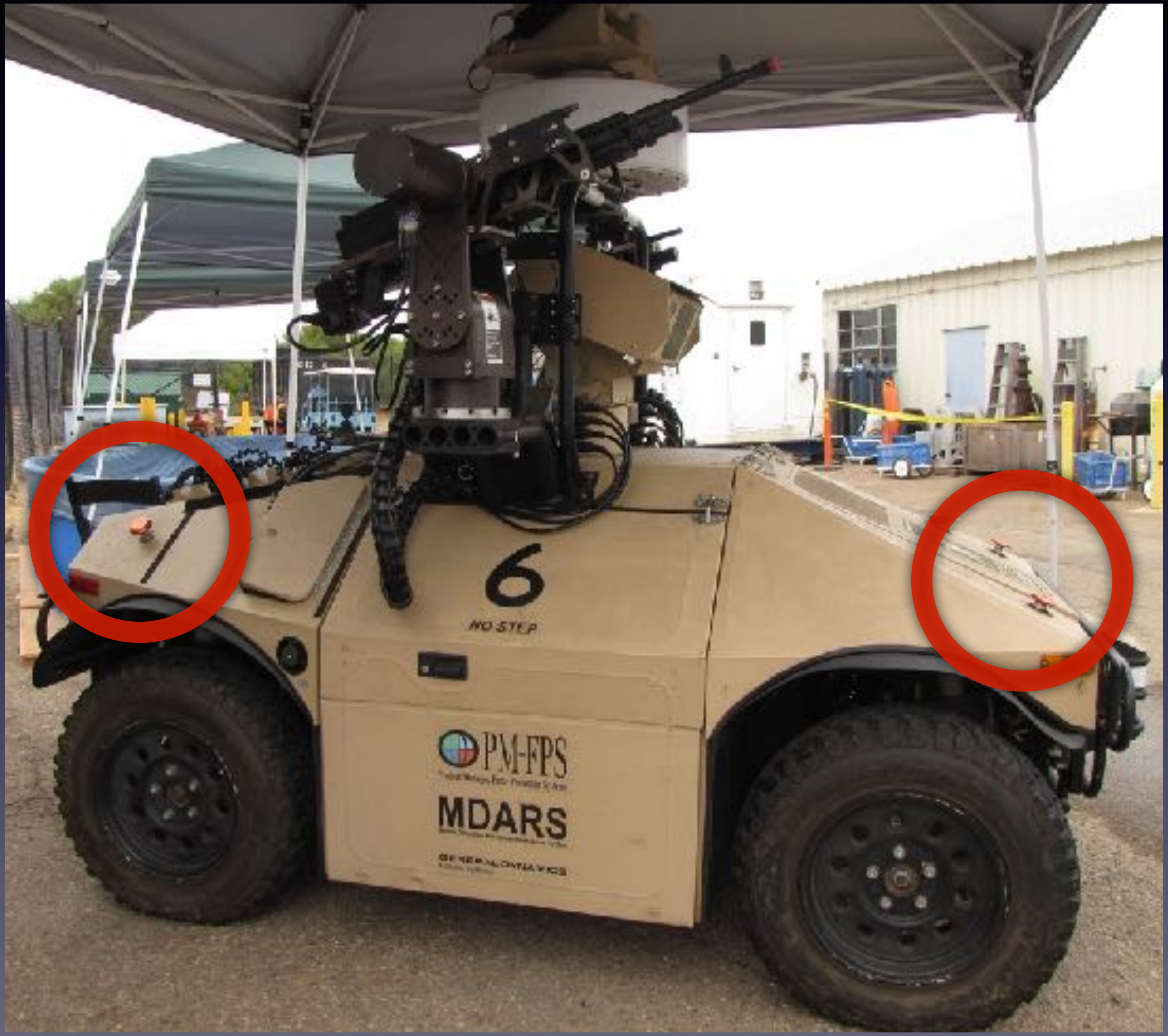
UAS Uptake

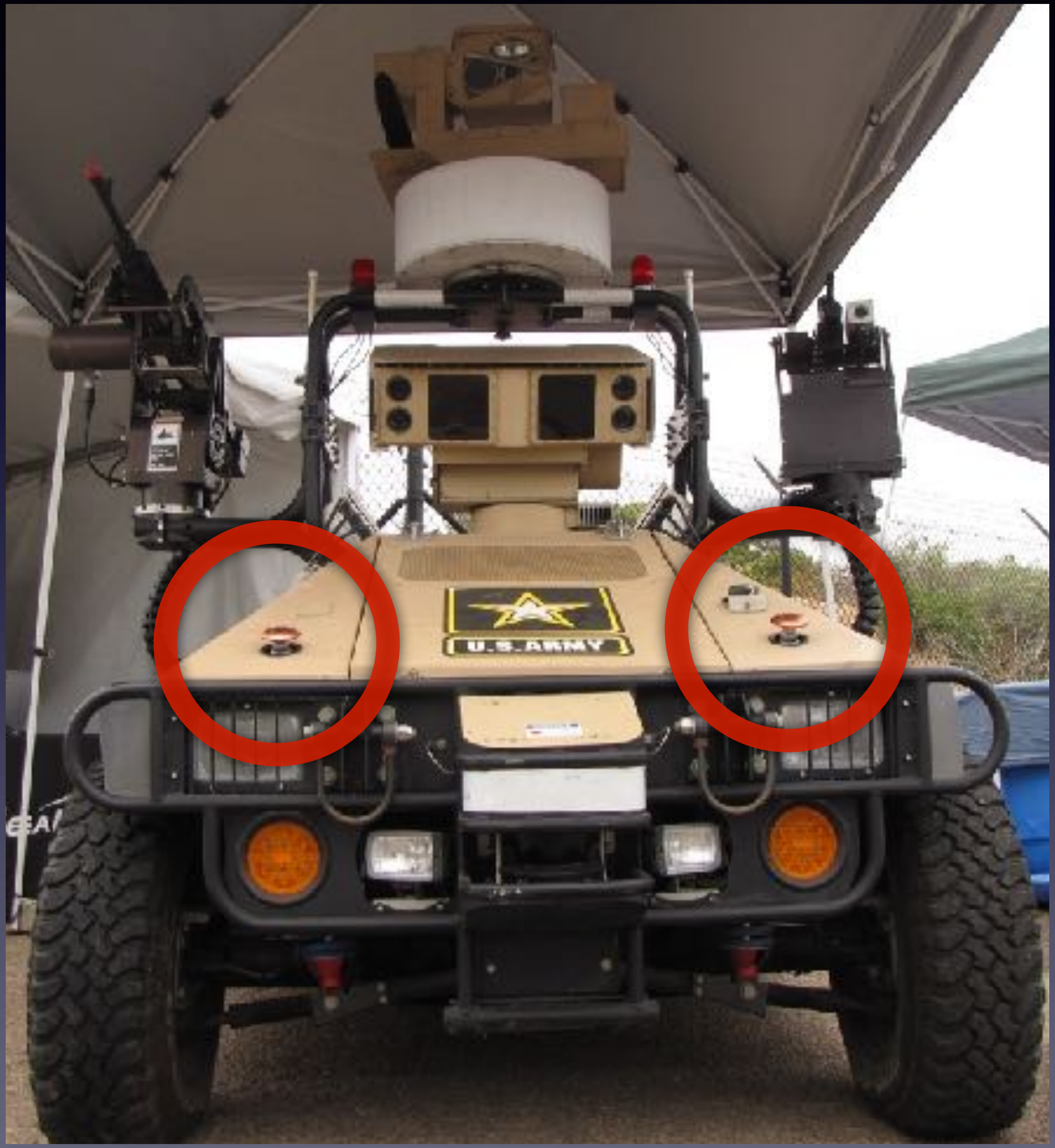


Northrop Grumman

"Unmanned Advanced Capability Aircraft and Ground Combat Vehicles
It shall be a goal of the Armed Forces to achieve the fielding of unmanned, remotely controlled technology such that by 2015, one-third of the operational ground combat vehicles of the Armed Forces are unmanned."
—*National Defense Authorization Act for Fiscal Year 2001* (S. 2549, Sec. 217)

Some UGVs are designed with threats in mind...





Civil Applications

Transportation

Oceanography

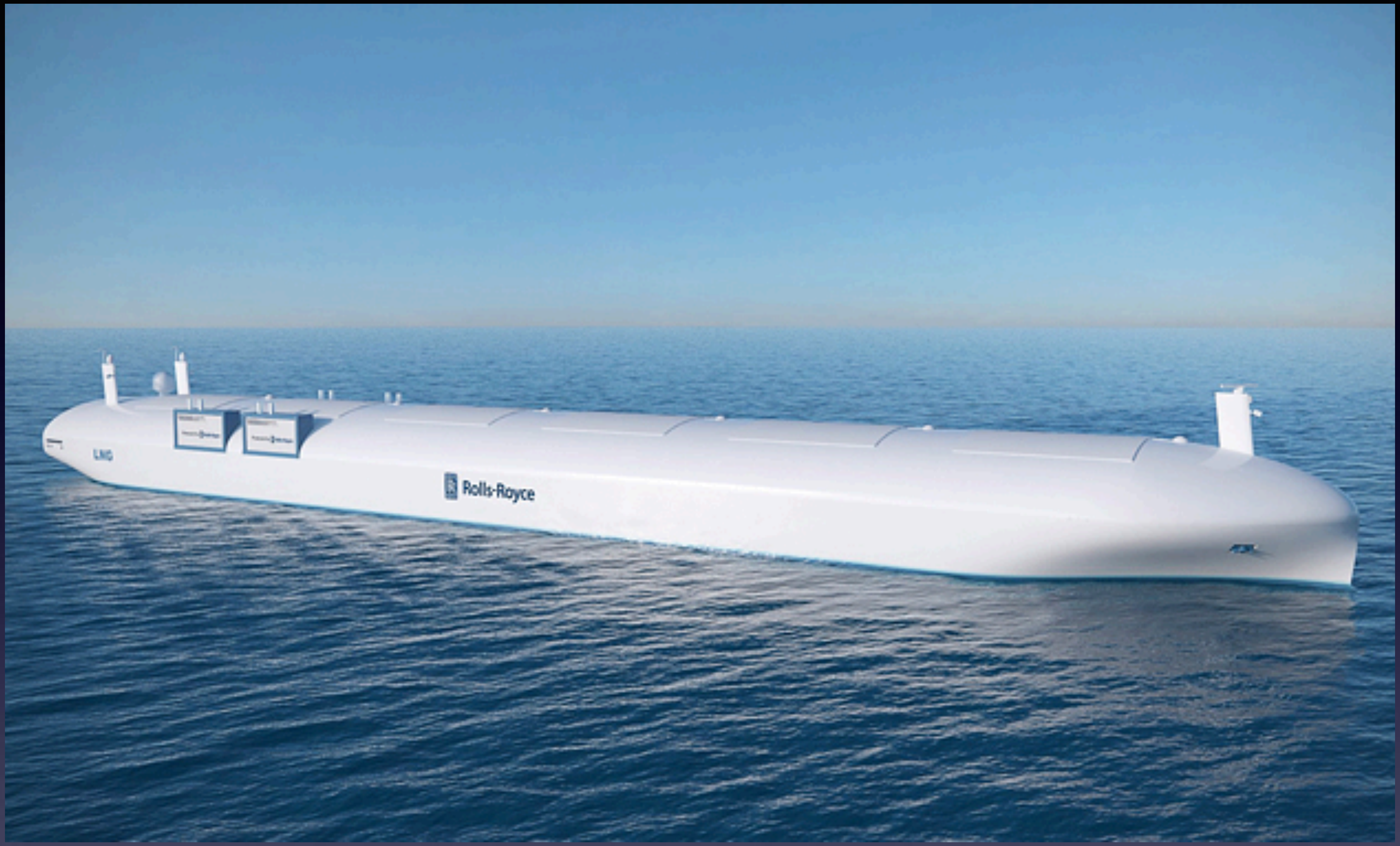
Mapping

Filmmaking

Powerline Inspection

Logistics

Civil Applications



- Unmanned cargo shipping
- 75% of maritime accidents caused by human error
- Major technical challenge: dealing with hardware failure on long voyages

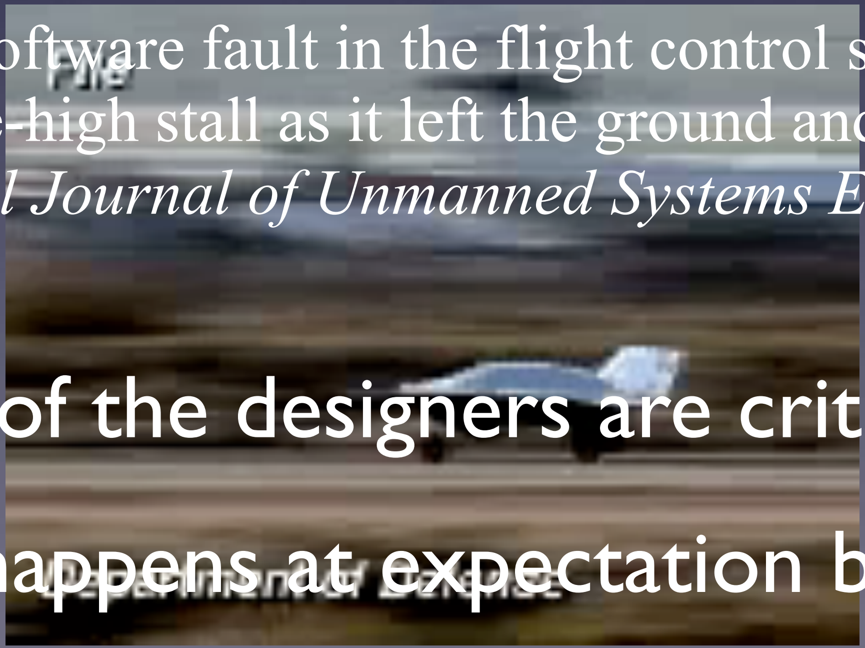
Civil Applications

- Priorities:
  - Precision Agriculture
  - Self-Driving Cars
- Roadblocks:
  - Shared Infrastructure (Airspace, Roads)
  - Acceptance (Safety, Robustness)
- Let's Talk Failure!

Classic Failures

RQ-3 DarkStar

$10m Unit Procurement Cost (Units 11-20, 1994 $)

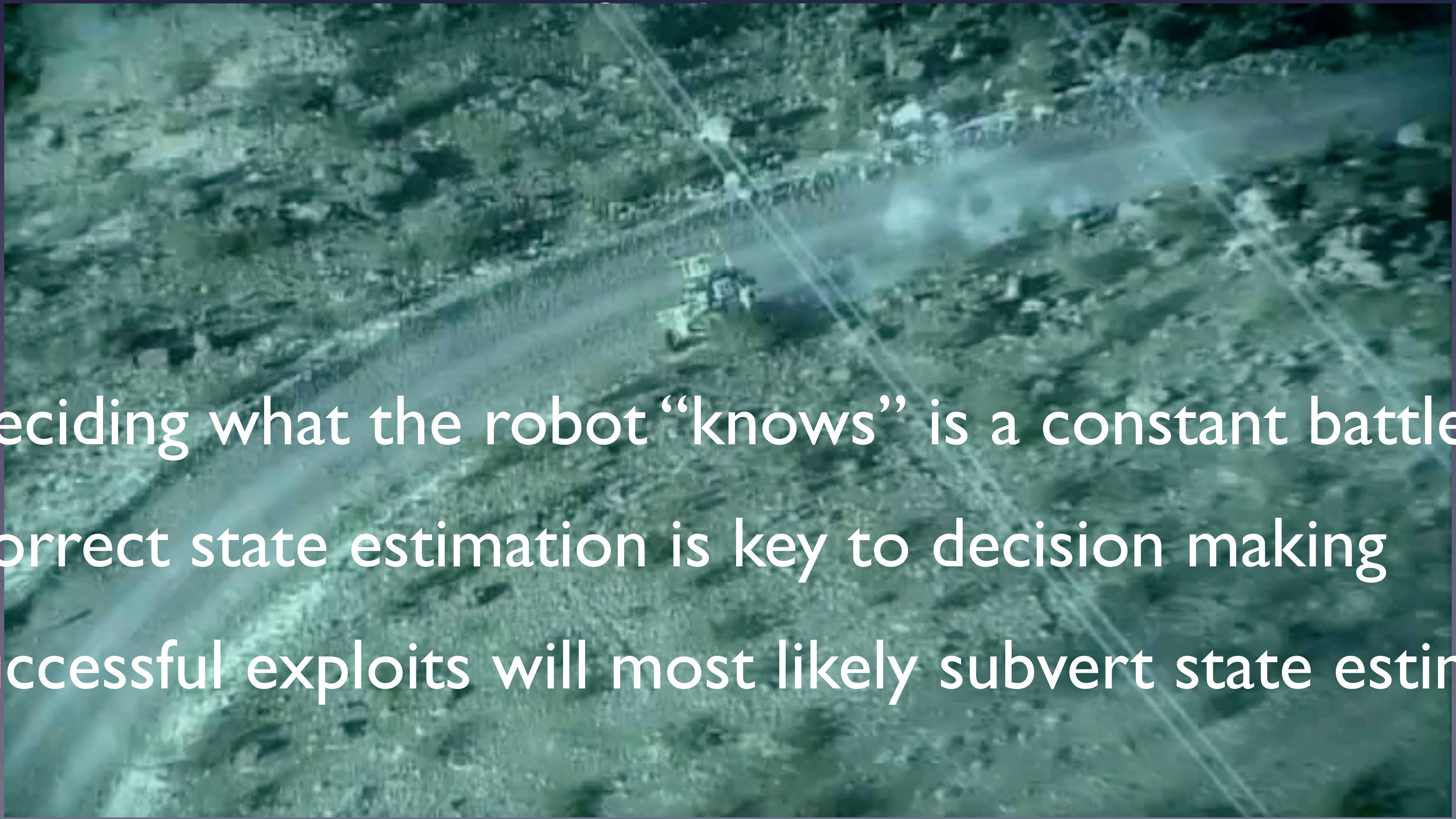


On its second flight, due to a software fault in the flight control system the aircraft's porpoising oscillations increased to a nose-high stall as it left the ground and the vehicle crashed.

—*International Journal of Unmanned Systems Engineering, Vol. 1, No. S3, 1–5*

- Expectations of the designers are critical!
- Exploitation happens at expectation boundary "cracks"

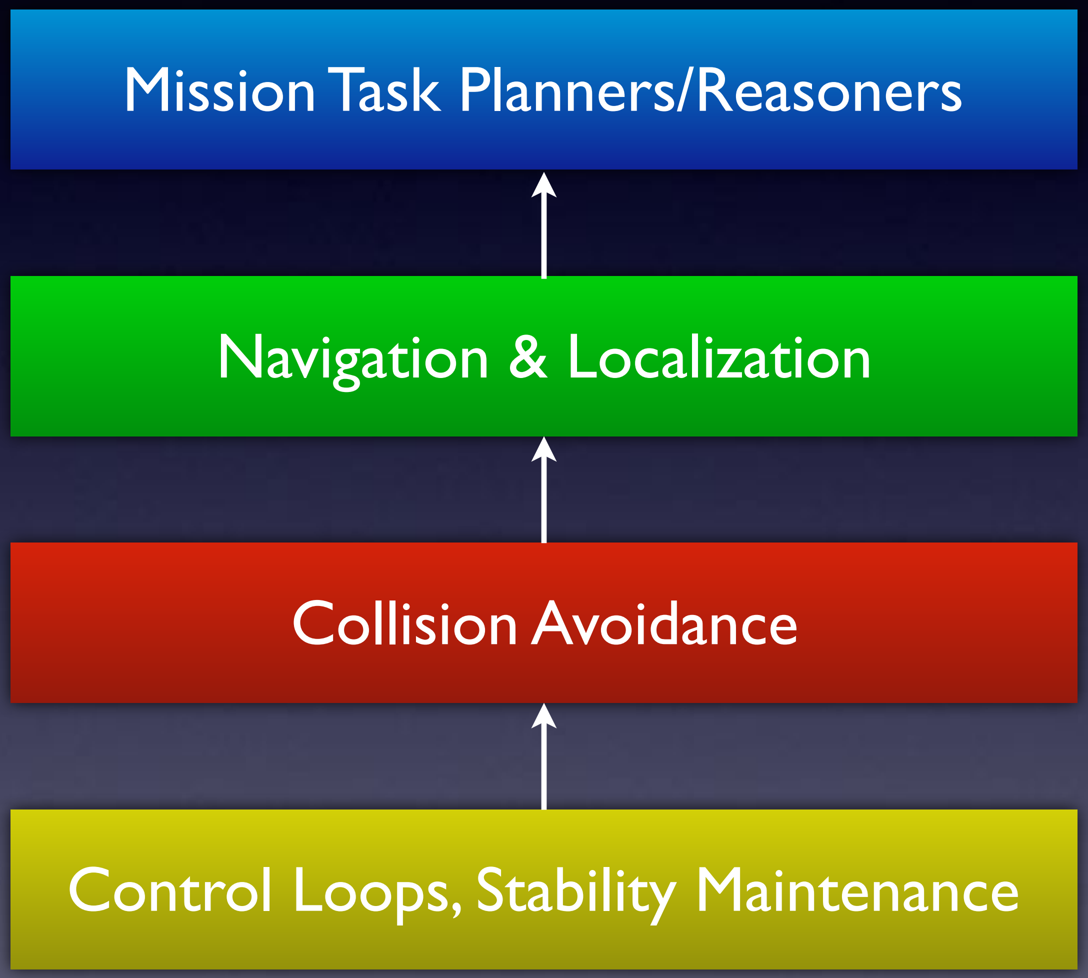
Classic Failures



- Deciding what the robot "knows" is a constant battle
- Correct state estimation is key to decision making
- Successful exploits will most likely subvert state estimation

Autonomous Vehicle Logic Structures

Activity Hierarchy



Mission Task Planners/Reasoners

Navigation & Localization

Collision Avoidance

Control Loops, Stability Maintenance

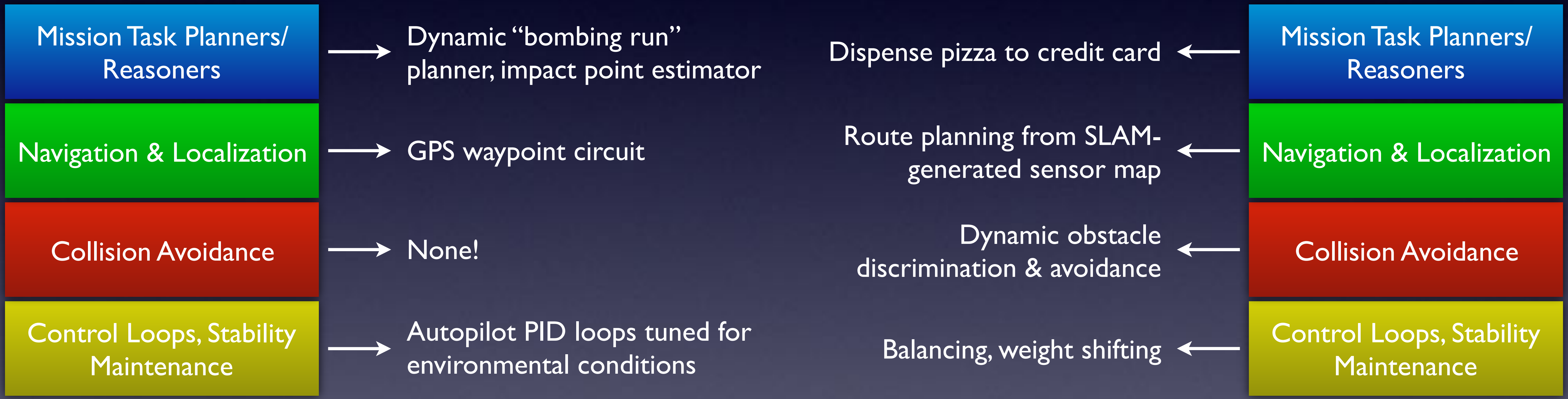
- Attacks lower in the stack defeat everything above
- More engineering effort spent on guaranteed robustness at lower levels
  - Lower layers may be juicier but harder targets

Autonomous Vehicle Logic Structures

Examples

Lifesaving Drone

Pizza Delivery



Mission Task Planners/ Reasoners → Dynamic "bombing run" planner, impact point estimator

Navigation & Localization → GPS waypoint circuit

Collision Avoidance → None!

Control Loops, Stability Maintenance → Autopilot PID loops tuned for environmental conditions

Dispense pizza to credit card ← Mission Task Planners/ Reasoners

Route planning from SLAM-generated sensor map ← Navigation & Localization

Dynamic obstacle discrimination & avoidance ← Collision Avoidance

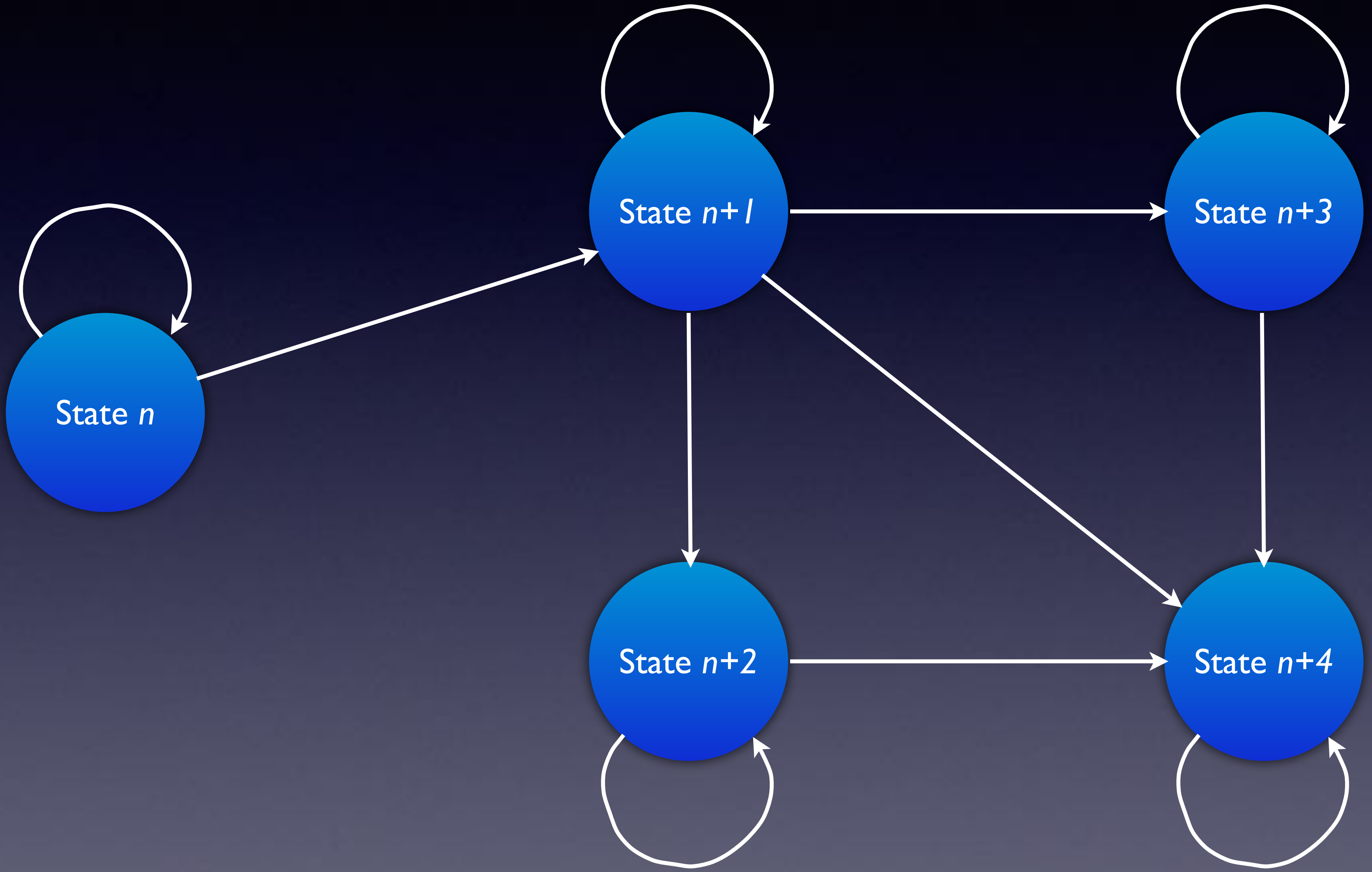
Balancing, weight shifting ← Control Loops, Stability Maintenance

- Extremely vulnerable to collision
- High level logic depends on single sensor

- Vulnerable to redirection, trapping and map-confusion attacks

Autonomous Vehicle Logic Structures

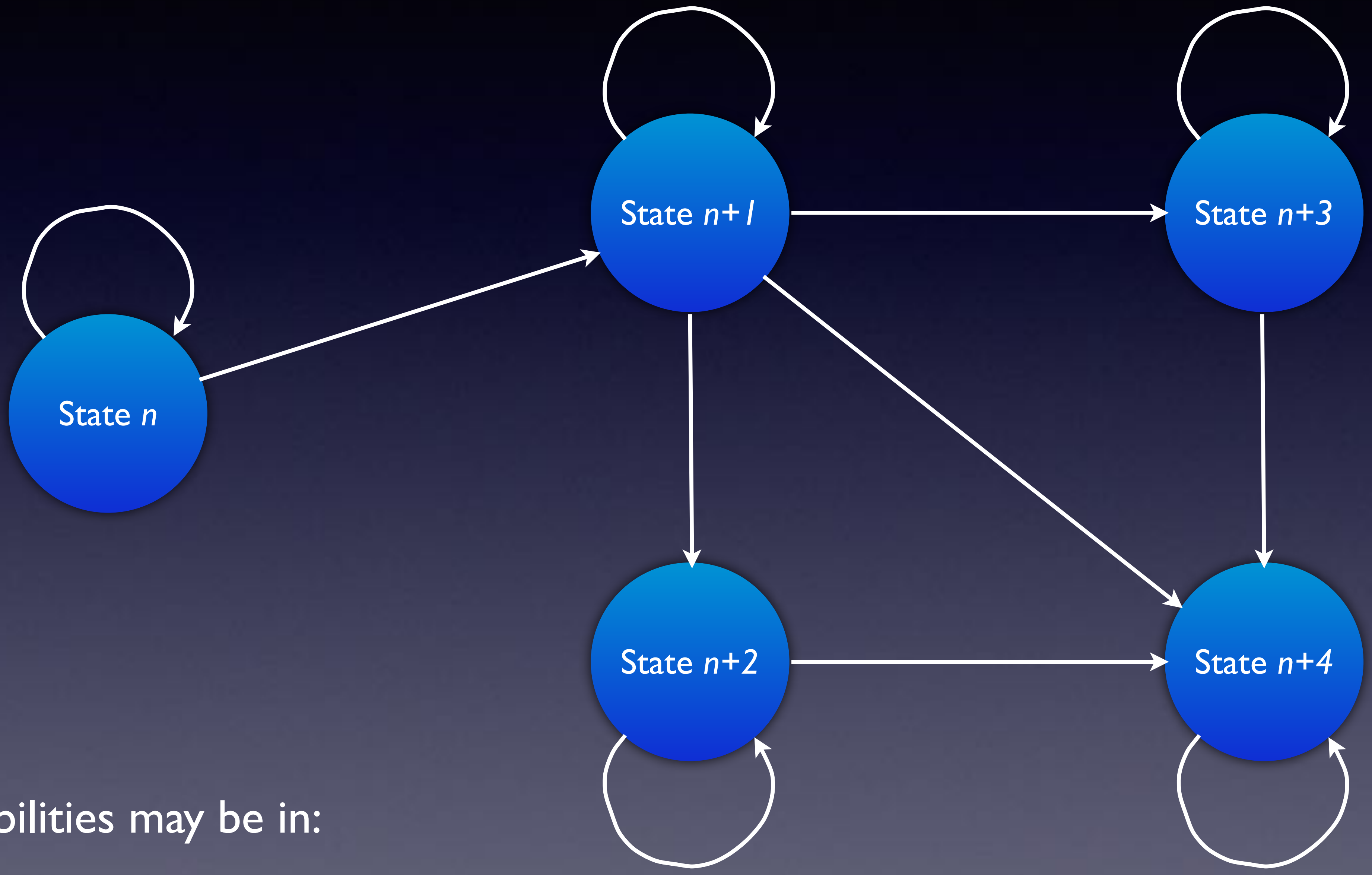
Mission Oriented State Machines



- States may correspond to tasks
- Transitions may be task completions, context switches or timeouts
- States may themselves contain state machines, reasoners, planners etc

Autonomous Vehicle Logic Structures

Mission Oriented State Machines

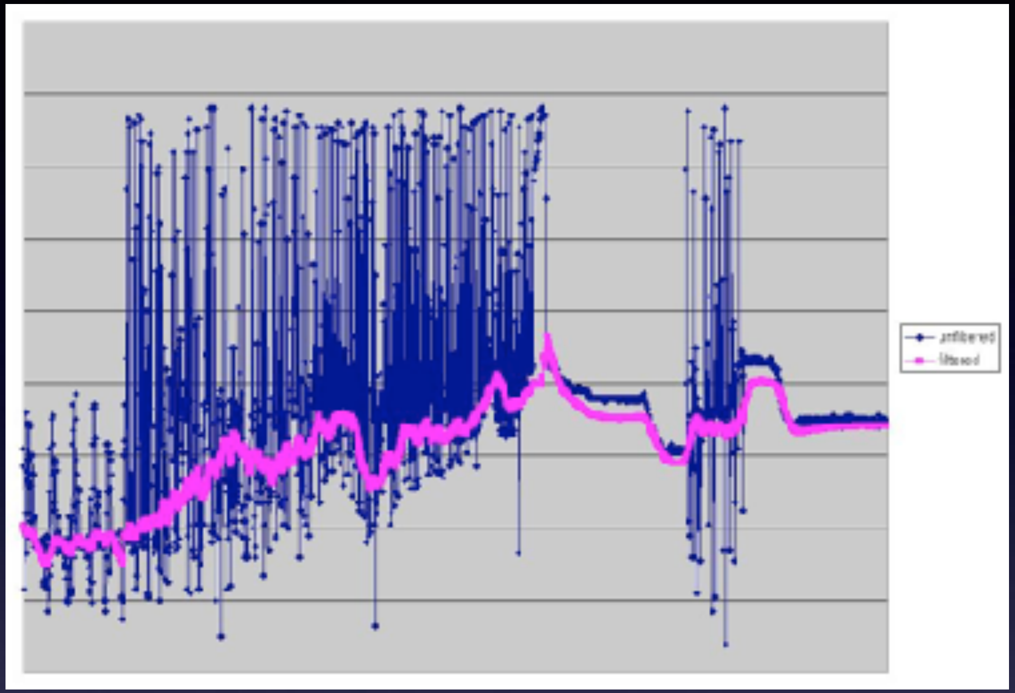


- Vulnerabilities may be in:
  - State estimation
  - Transitions (spoofing or preventing)
  - Unexpected conditions within states

Sensors

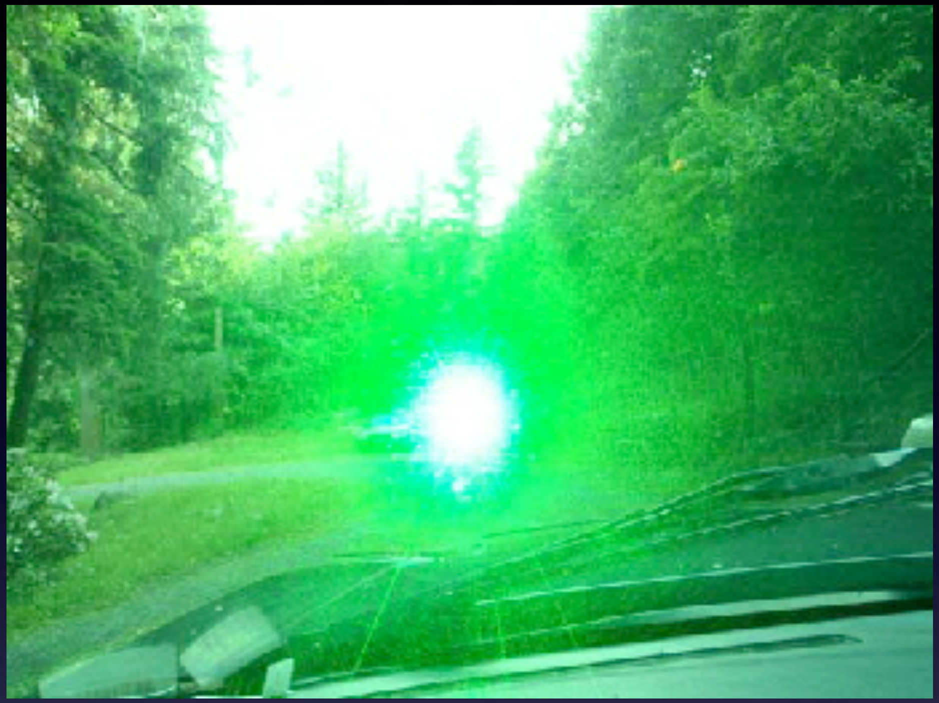
- Active vs Passive
- Common sensors:
  - GPS
  - LIDAR
  - Cameras
  - Millimeter Wave Radar
  - Ultrasonic Transducers
  - Digital Compass
  - IMU
  - Wheel Encoders
  - Doppler Velocity Logger (subsurface)
  - Scanning SONAR (subsurface)
  - Pressure Transducers (air & subsurface)

Sensors



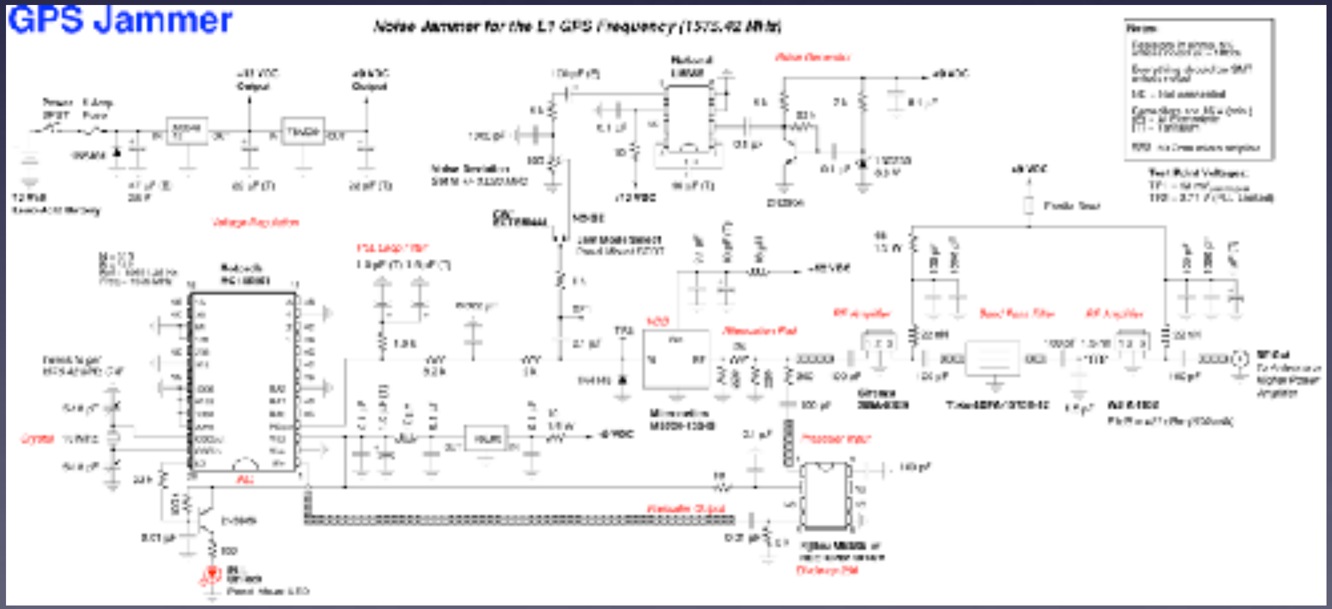
- Sources of uncertainty:
    - Noise
    - Drift
    - Latency & update rate
- Uncertainty must be modeled under assumptions
- Sensor fusion:
    - Fused/registered data can be more useful than separate
    - What to do when sensors disagree?
- Robot robustness may come down to:
    - How smart is it at discounting 1 bad/spoofed sensor?

Sensor Attacks



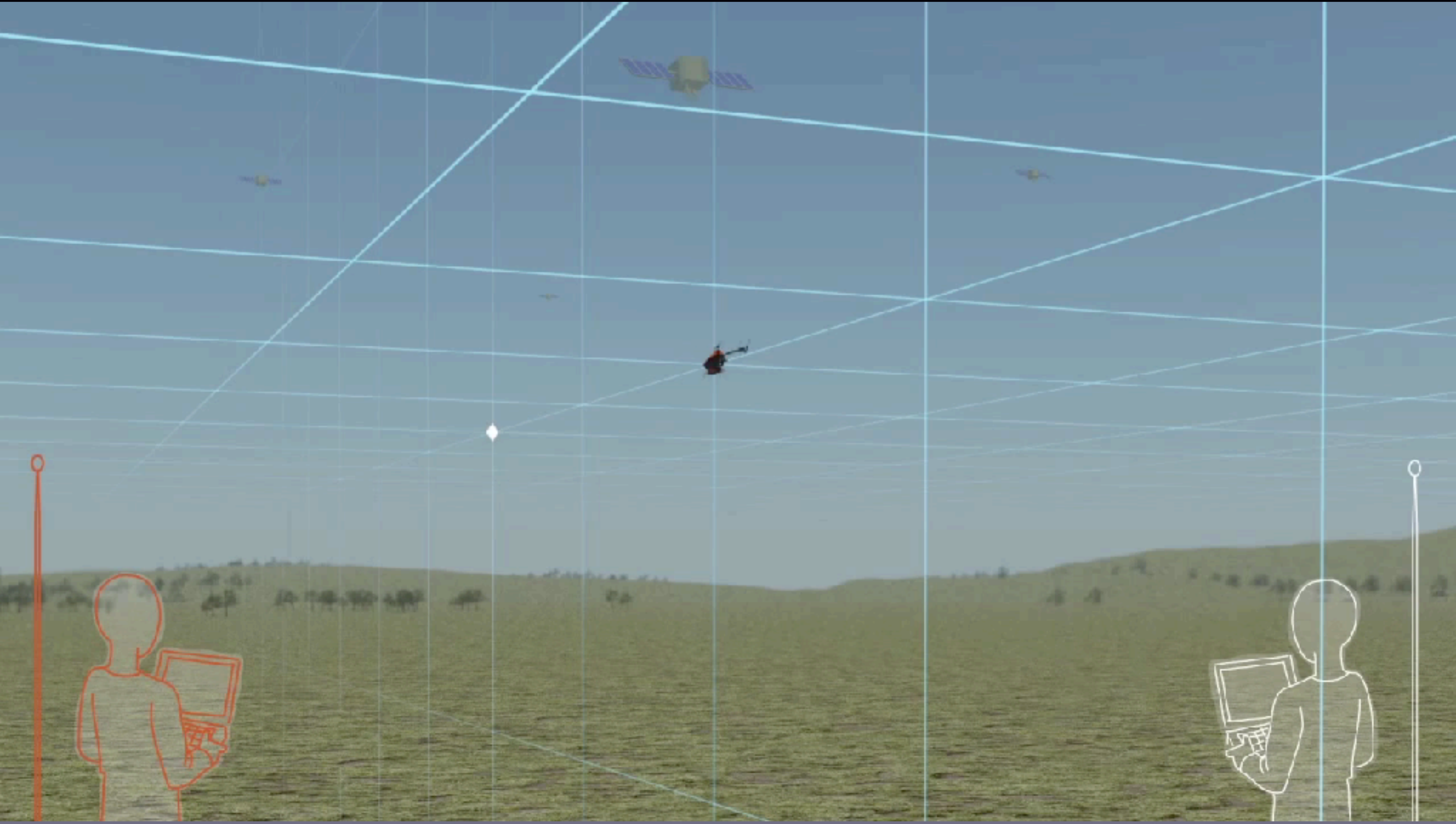
- 2 kinds:
    - Denial
        - Preventing sensor from recovering useful data
    - Spoofing
        - Causing sensor to retrieve specifically incorrect data
- Basic attack mode choice:
    - Attack sensors instantaneously
    - Attack aggregated sensor data

GPS



- Denial:
  - Jamming
- Spoofing:
  - Fake GPS satellite signals at higher power

GPS



اسرائیل باید از صحنه روزگار محو شود
Israel must be wiped out of the scene
آمریکا هیچ غلطی نمی تواند بکند
American Can Do No Wrong

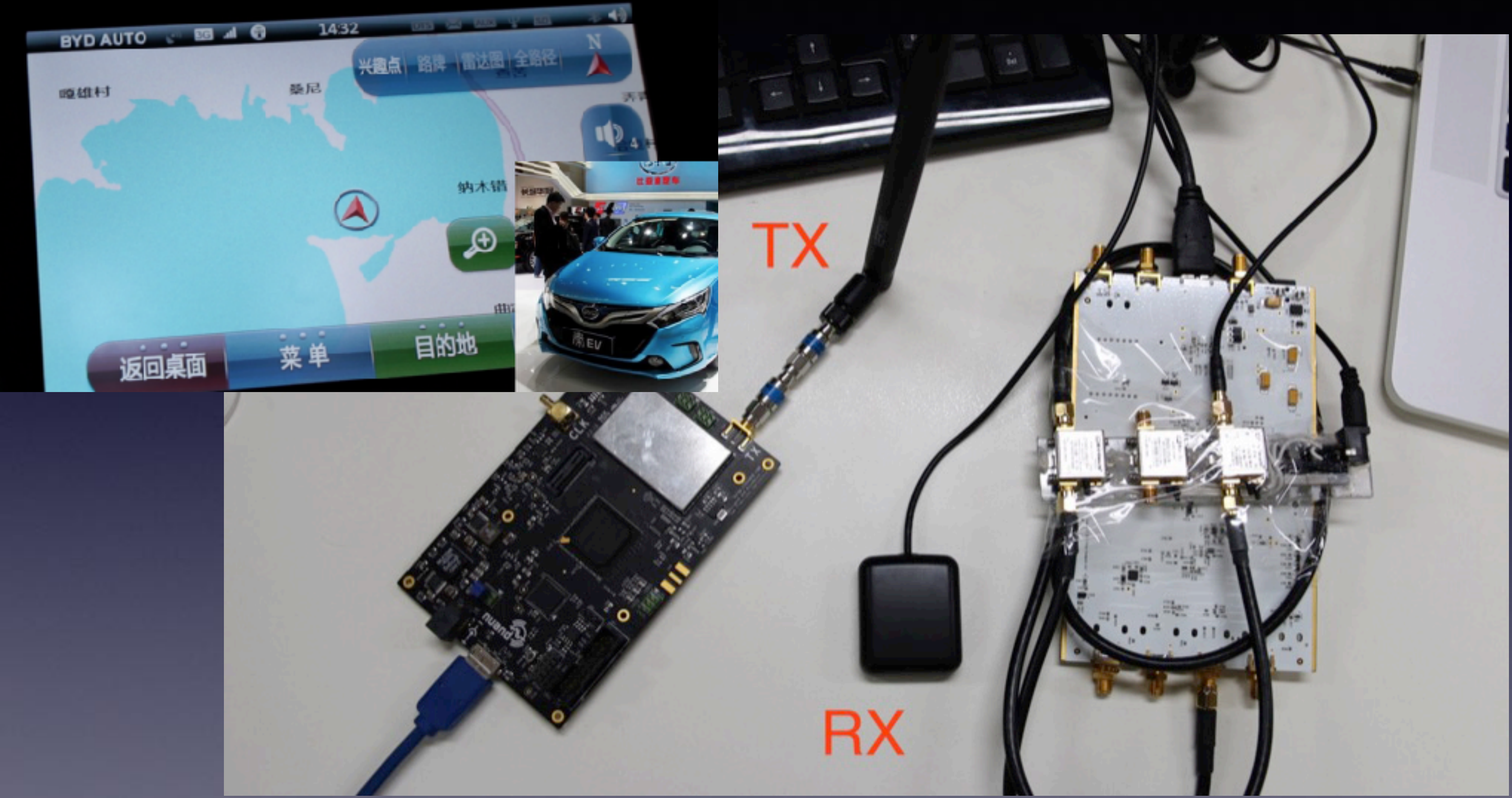
مرگ بر آمری
RQ170 – هواپیمای پیشرفته جاسوسی آمریکا
تسلط مدافعان ایران اسلامی بر تحرکات شیطان بزرگ
اخبار شبکه یک

NOVA

02
MY RIDE

GPS

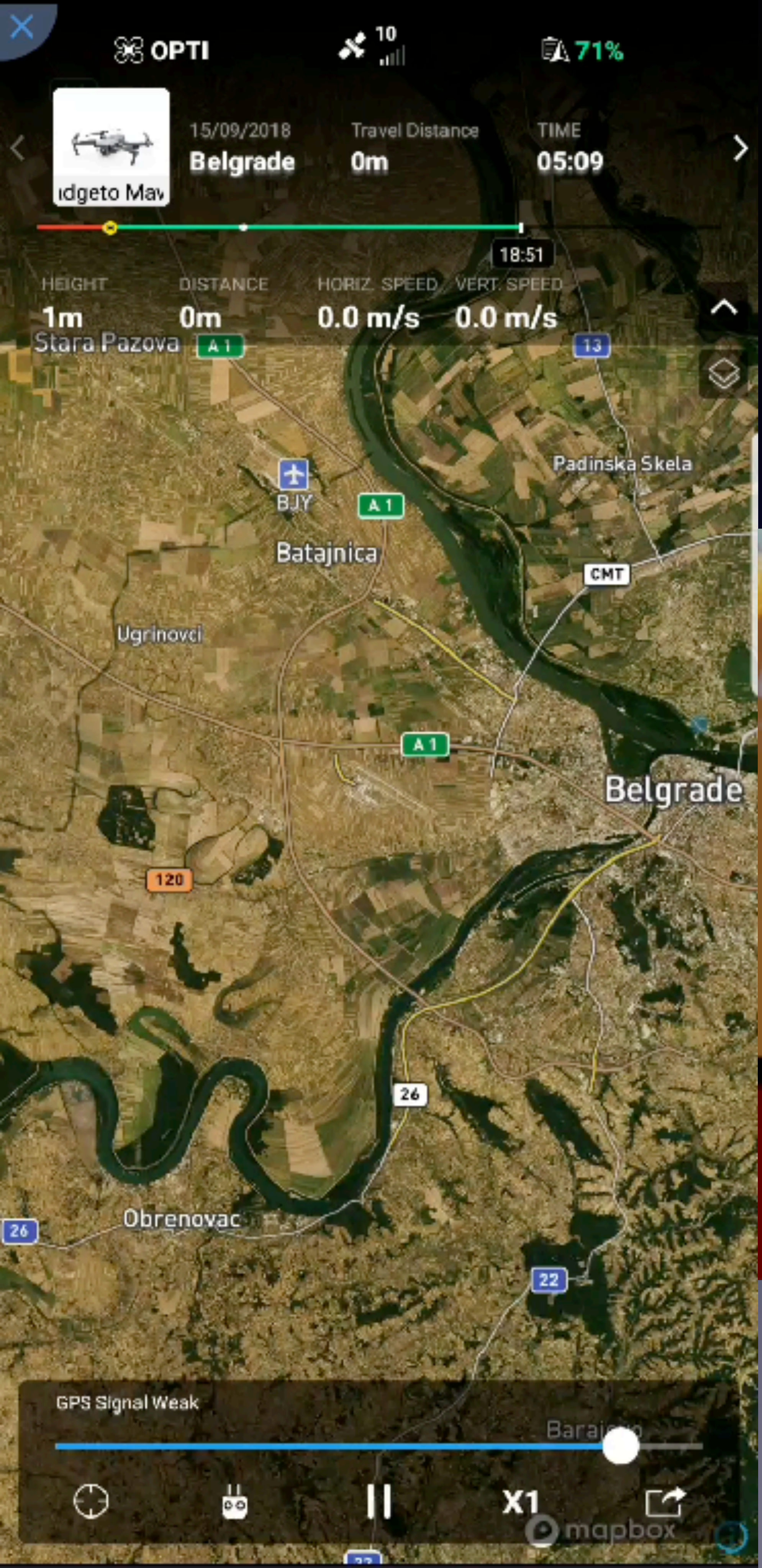
GPS



- Low Cost GPS Simulator Using BladeRF SDR
  - Qihoo360 Unicorn Team Huang & Yang, DEF CON 23

Demo Time

UAV Takedown!



OPTI 10 71%

Gadgeto Mav

15/09/2018
Belgrade

Travel Distance
0m

TIME
05:09

18:51

HEIGHT 1m

DISTANCE 0m

HORIZ. SPEED 0.0 m/s

VERT. SPEED 0.0 m/s

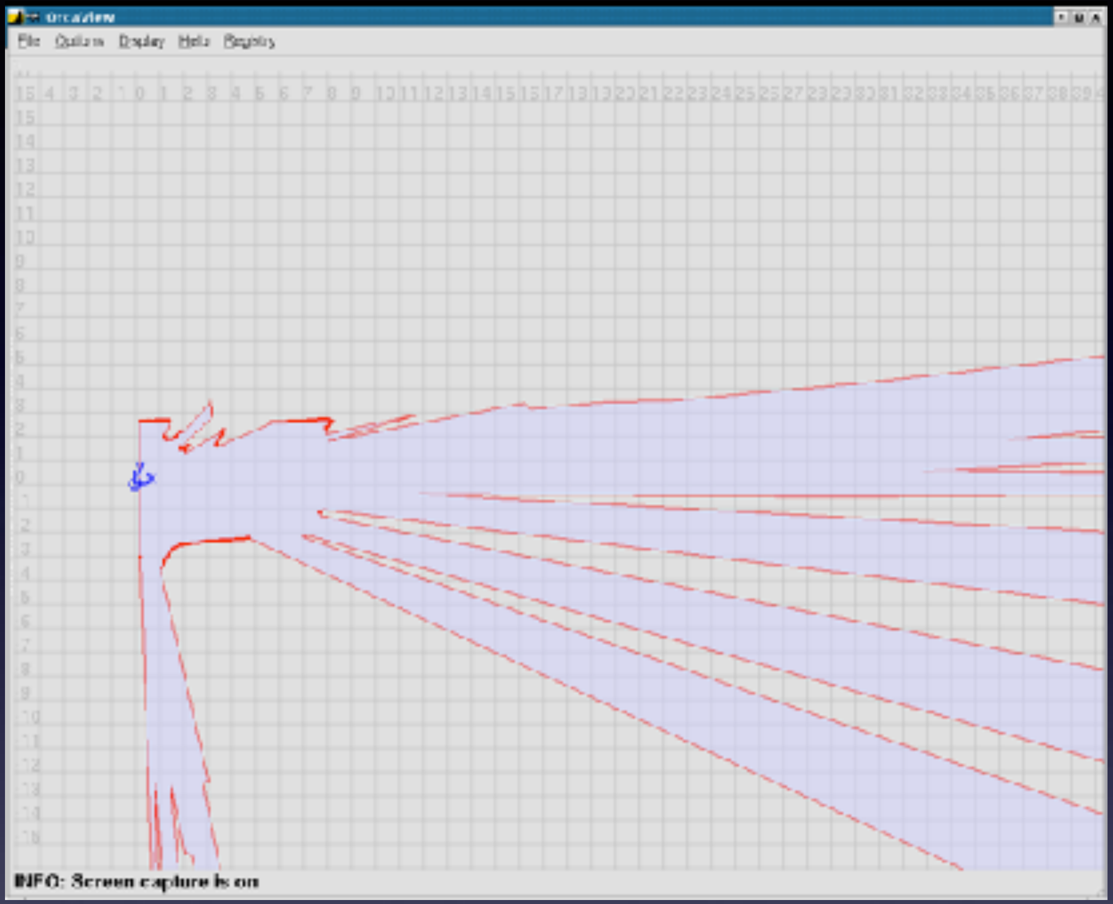
GPS Signal Weak

X1

LIDAR

- Originally industrial monitoring sensors
- Mechanically scanned operation
- Primarily for collision avoidance & map building
- Denial:
  - Active overpowering
  - Preventing return signal
- Spoofing:
  - Manipulating absorbence/reflectivity
  - Active spoofing

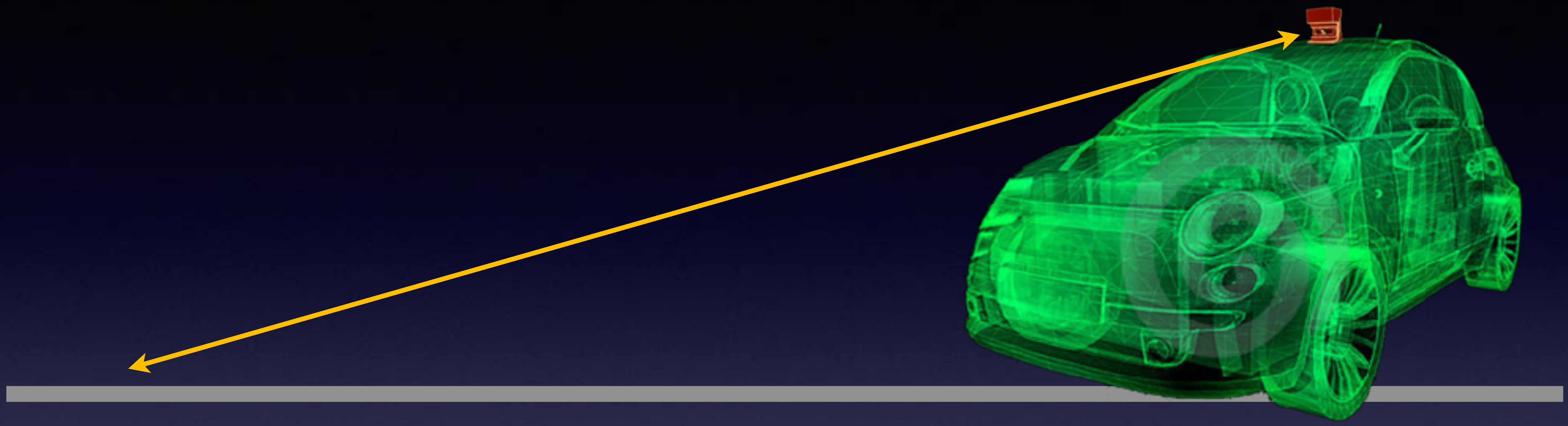
LIDAR



INFO: Screen capture is on

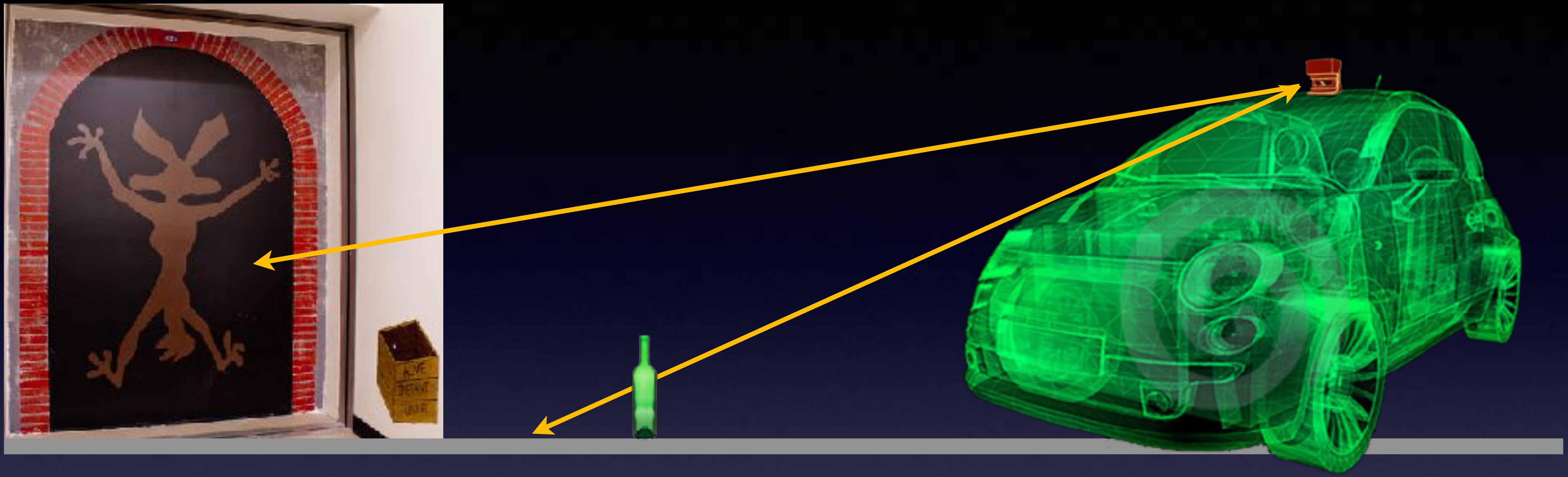
- 2D sensor highly orientation dependent
  - Inclines can look like obstacles
  - May miss low obstacles & discontinuities

LIDAR



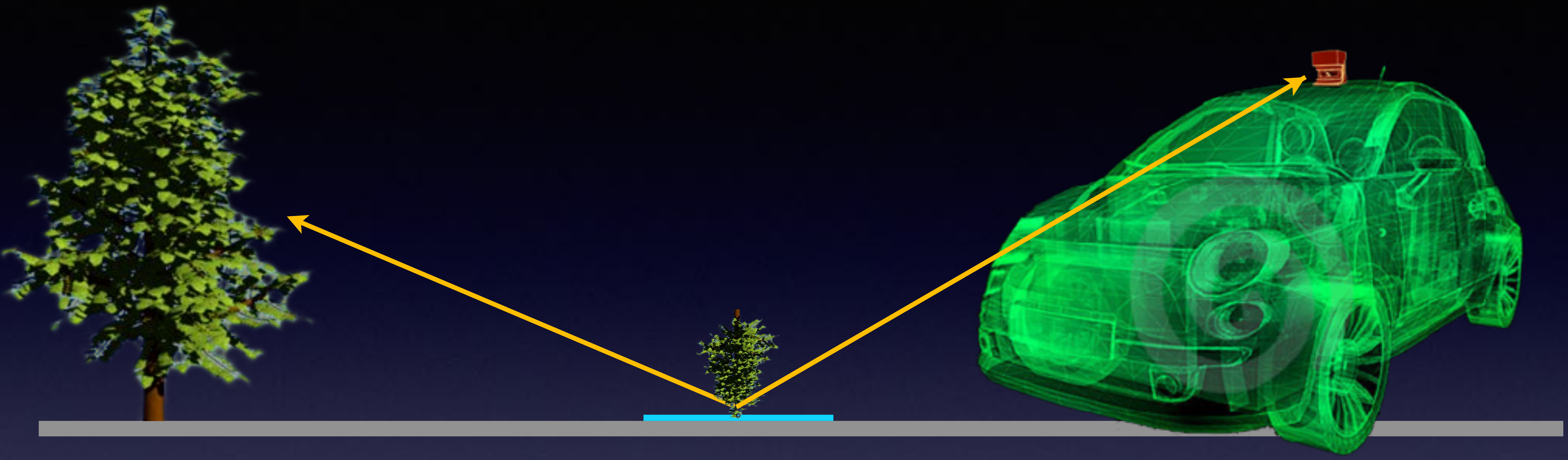
- Active emission sensor
  - Can only see what returns a signal
  - No return = nothing there
  - Most of the world returns no data

LIDAR



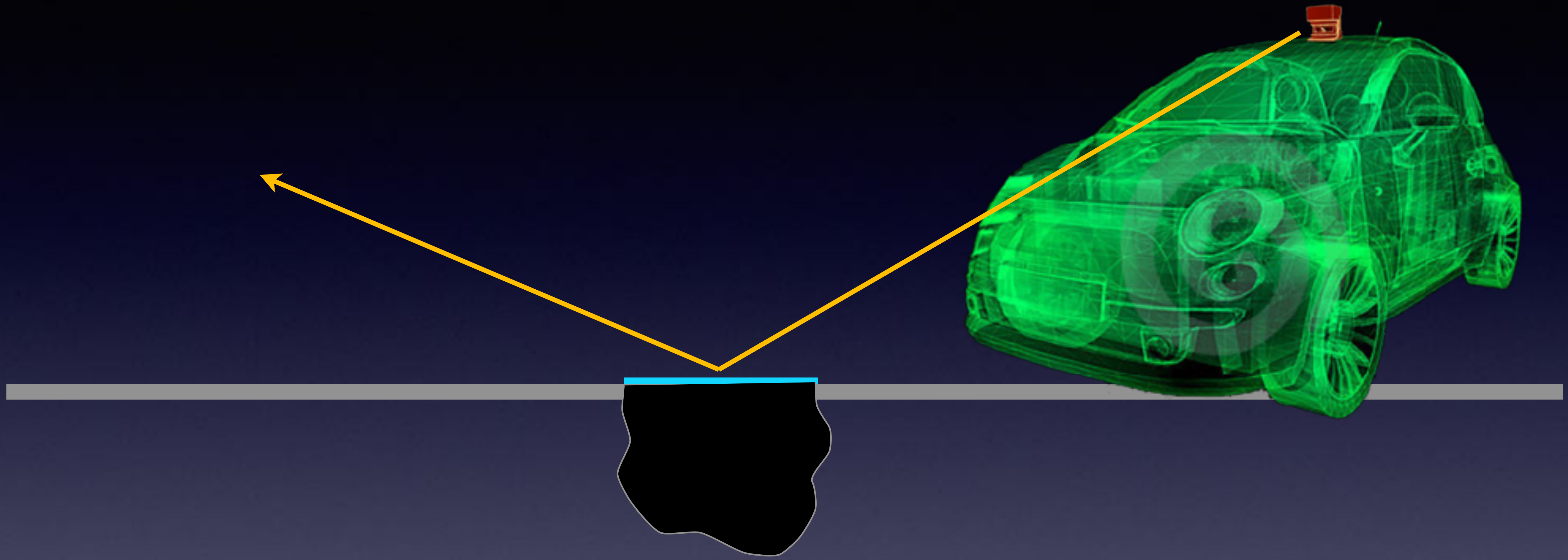
- Absorbent things look like nothing
  - Also transparent

LIDAR



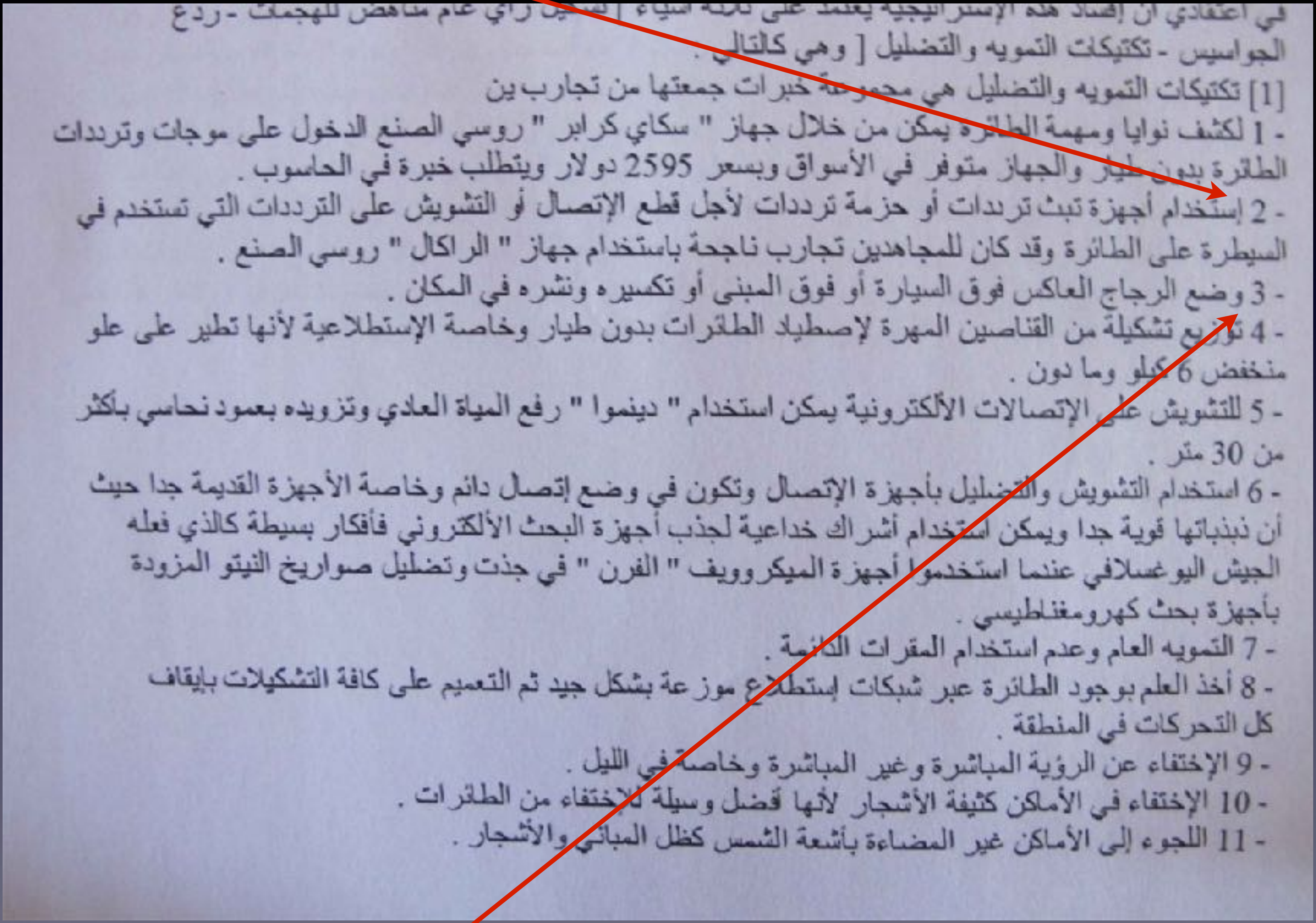
- Reflective things can confuse laser
  - Faraway things brought near
  - Loss of return looks like ditch

LIDAR



- Reflective things can confuse laser
  - Faraway things brought near
  - Loss of return looks like ditch

Russian “Racal” GPS jammer



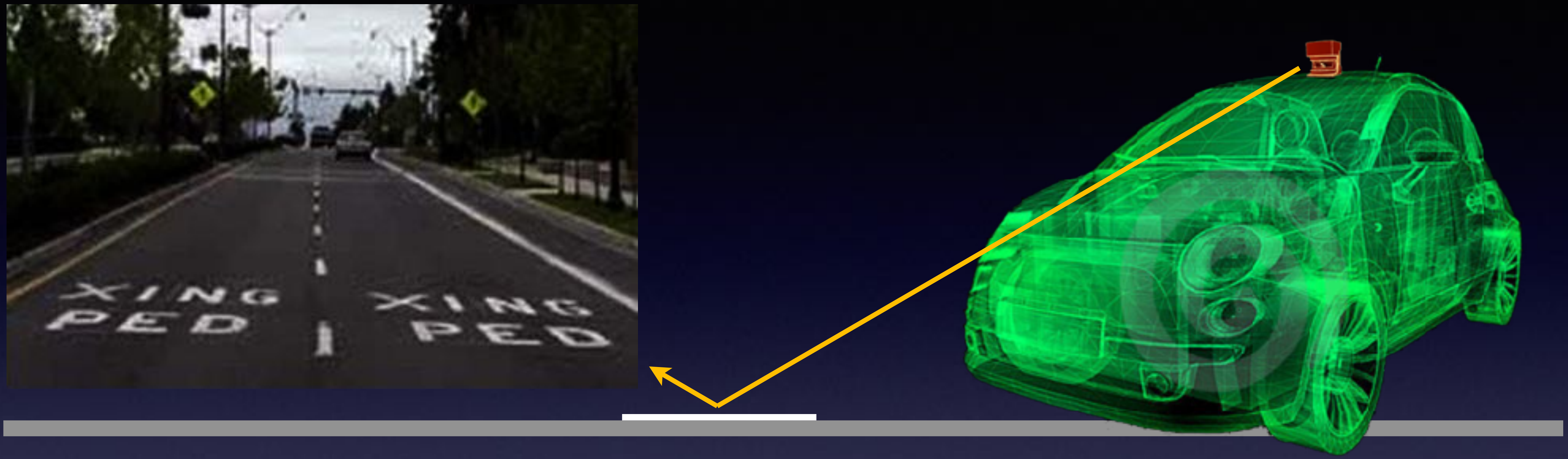
في اعتقادي أن إفساد هذه الإستراتيجية يعتمد على ثلاثة أشياء [تشكيل رأي عام مناهض للهجمات - ردع
الجواسيس - تكتيكات التمويه والتضليل] وهي كالتالي .

[1] تكتيكات التمويه والتضليل هي مجموعة خبرات جمعتها من تجارب ين

- 1 لكشف نوايا ومهمة الطائرة يمكن من خلال جهاز " سكاي كرابر " روسي الصنع الدخول على موجات وترددات الطائرة بدون طيار والجهاز متوفر في الأسواق وبسعر 2595 دولار ويتطلب خبرة في الحاسوب .
- 2 إستخدام أجهزة تبث ترددات أو حزمة ترددات لأجل قطع الإتصال أو التشويش على الترددات التي تستخدم في السيطرة على الطائرة وقد كان للمجاهدين تجارب ناجحة باستخدام جهاز " الراكال " روسي الصنع .
- 3 وضع الرجاج العاكس فوق السيارة أو فوق المبنى أو تكسيره ونشره في المكان .
- 4 توزيع تشكيلة من القناصين المهرة لإصطياد الطائرات بدون طيار وخاصة الإستطلاعية لأنها تطير على علو منخفض 6 كيلو وما دون .
- 5 للتشويش على الإتصالات الألكترونية يمكن استخدام " دينموا " رفع المياة العادي وتزويده بعمود نحاسي بأكثر من 30 متر .
- 6 استخدام التشويش والتضليل بأجهزة الإتصال وتكون في وضع إتصال دائم وخاصة الأجهزة القديمة جدا حيث أن ذبذباتها قوية جدا ويمكن استخدام أشراك خداعية لجذب أجهزة البحث الألكتروني فأفكار بسيطة كالذي فعله الجيش اليوغسلافي عندما استخدموا أجهزة الميكروويف " الفرن " في جذت وتضليل صواريخ النيتو المزودة بأجهزة بحث كهرومغناطيسي .
- 7 التمويه العام وعدم استخدام المقرات الدائمة .
- 8 أخذ العلم بوجود الطائرة عبر شبكات إستطلاع موزعة بشكل جيد ثم التعميم على كافة التشكيلات بإيقاف كل التحركات في المنطقة .
- 9 الإختفاء عن الرؤية المباشرة وغير المباشرة وخاصة في الليل .
- 10 الإختفاء في الأماكن كثيفة الأشجار لأنها قضل وسيلة للإختفاء من الطائرات .
- 11 اللجوء إلى الأماكن غير المضاءة بأشعة الشمس كظل المباني والأشجار .

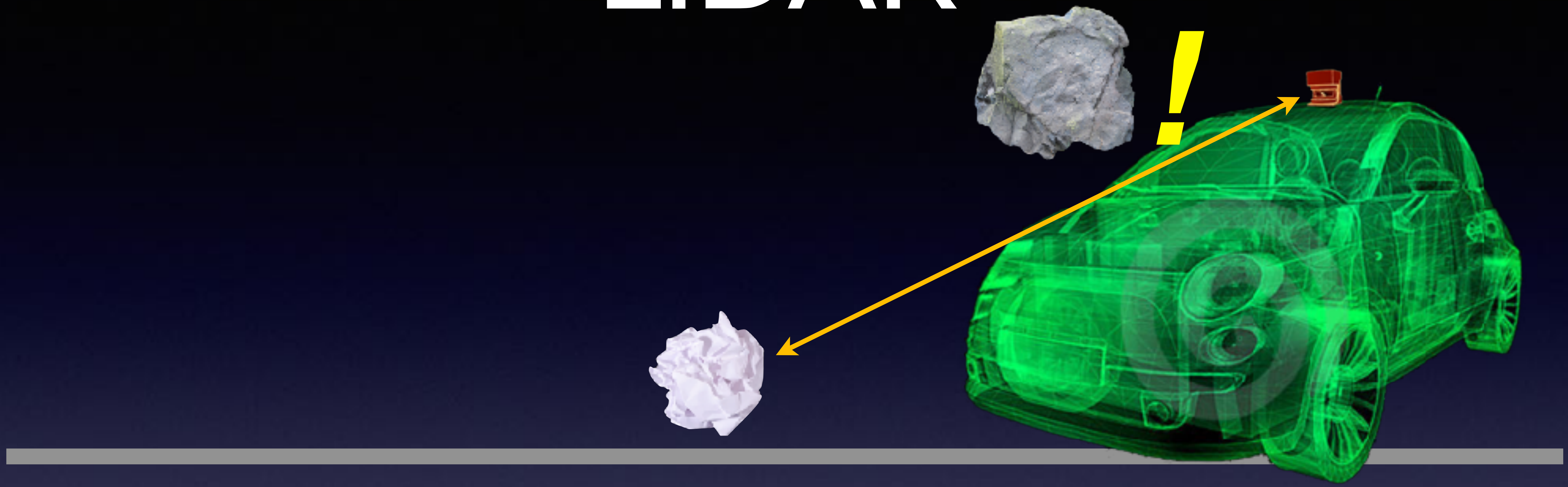
Use of reflective materials
to thwart laser designators

LIDAR



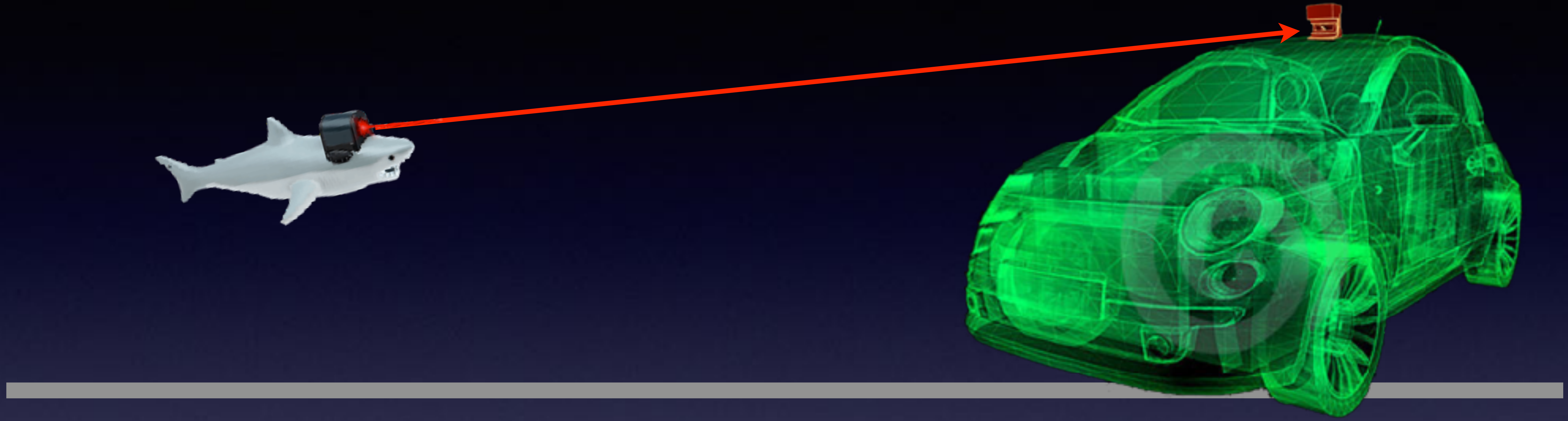
- Reflectance is also a feature
  - Road line detection
  - Can fake road markings invisibly to human

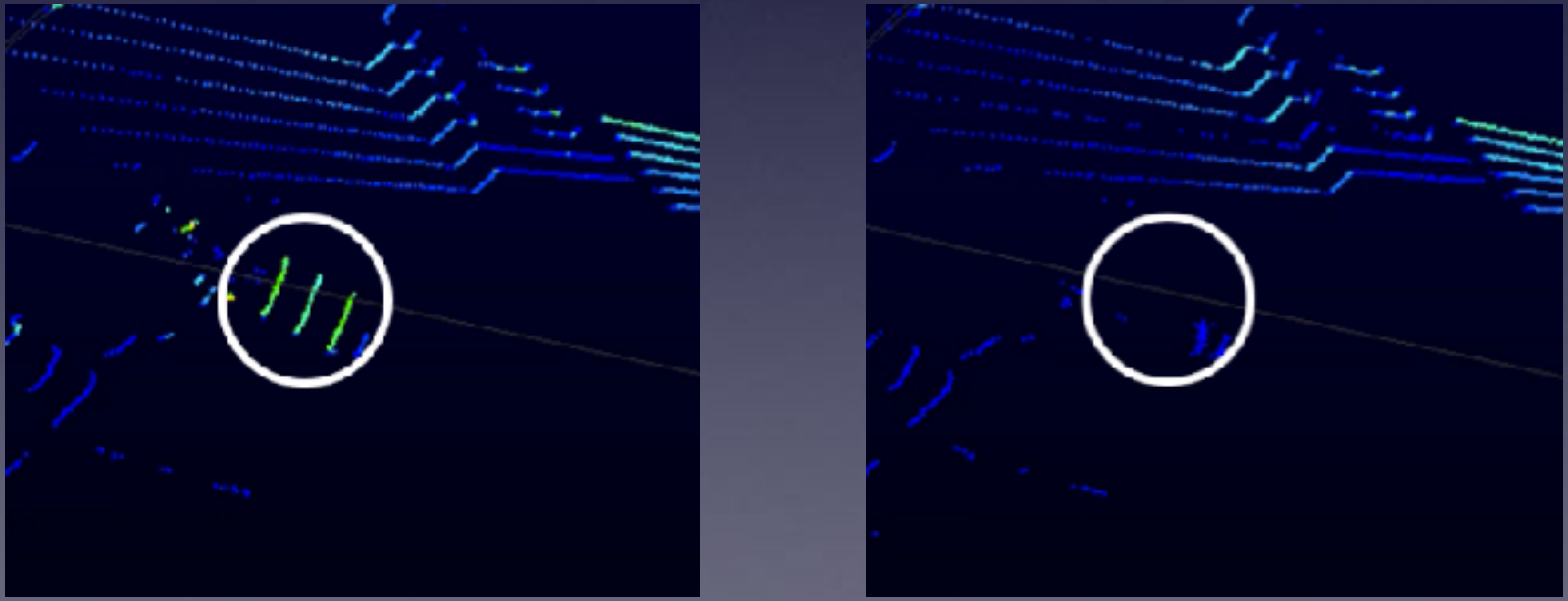
LIDAR



- Solid looking objects look solid

LIDAR

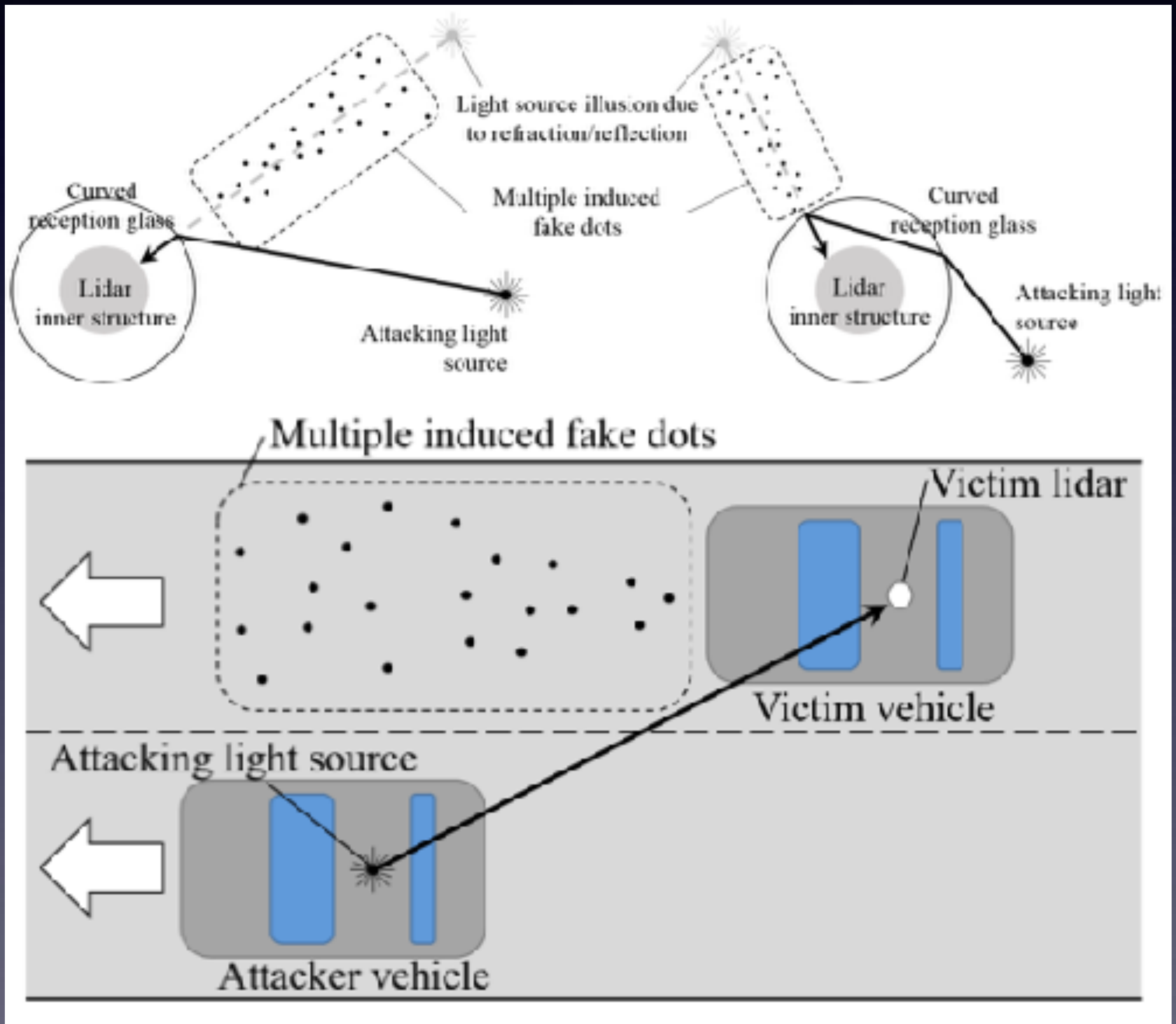




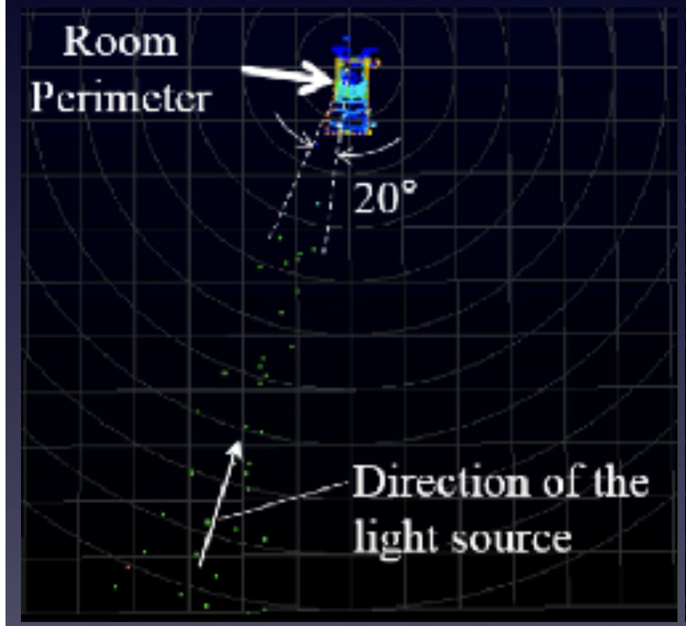
Shin, Kim, Kwon, Kim, KAIST, 2017

- Denial: strong source overpowers LIDAR in a certain area

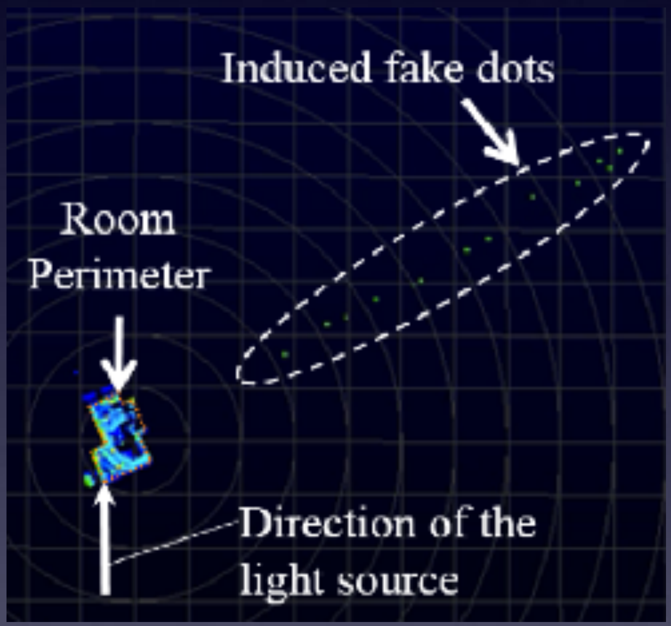
LIDAR



WEAK



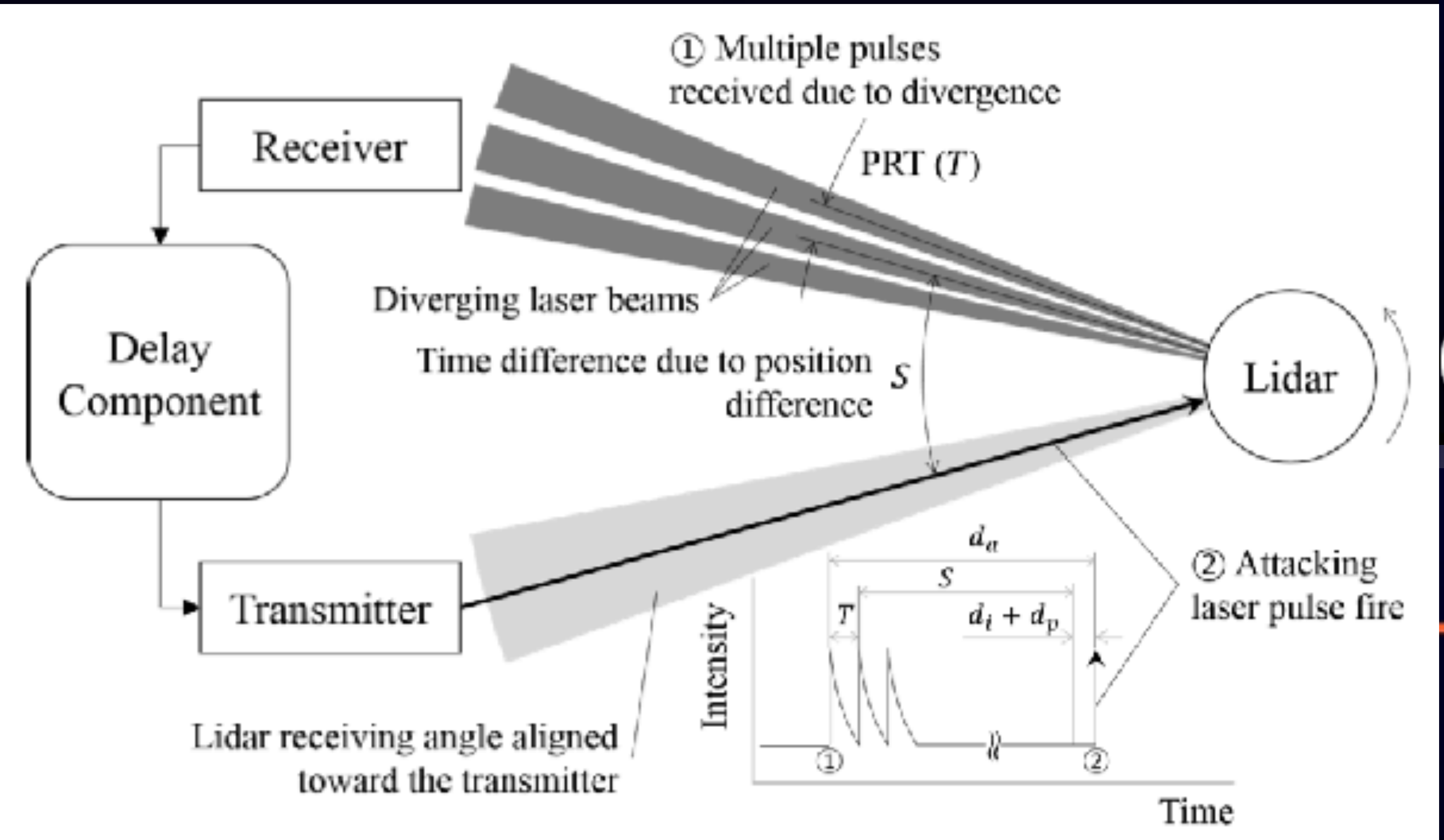
STRONG



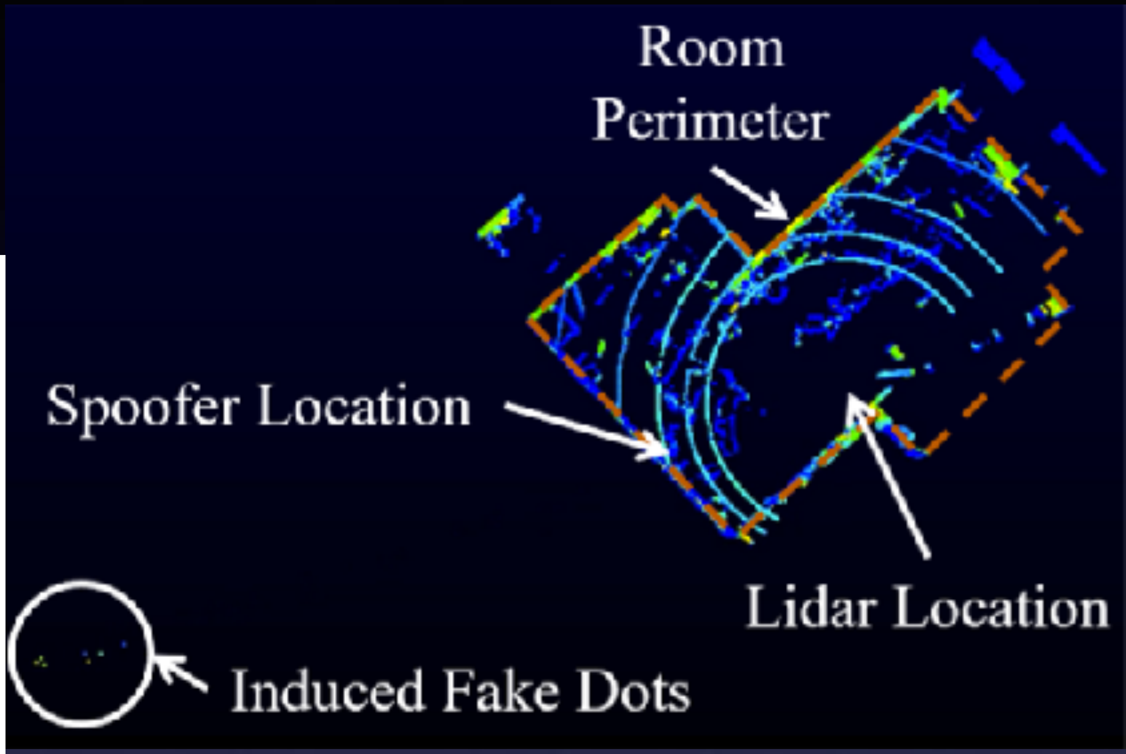
Shin, Kim, Kwon, Kim, KAIST, 2017

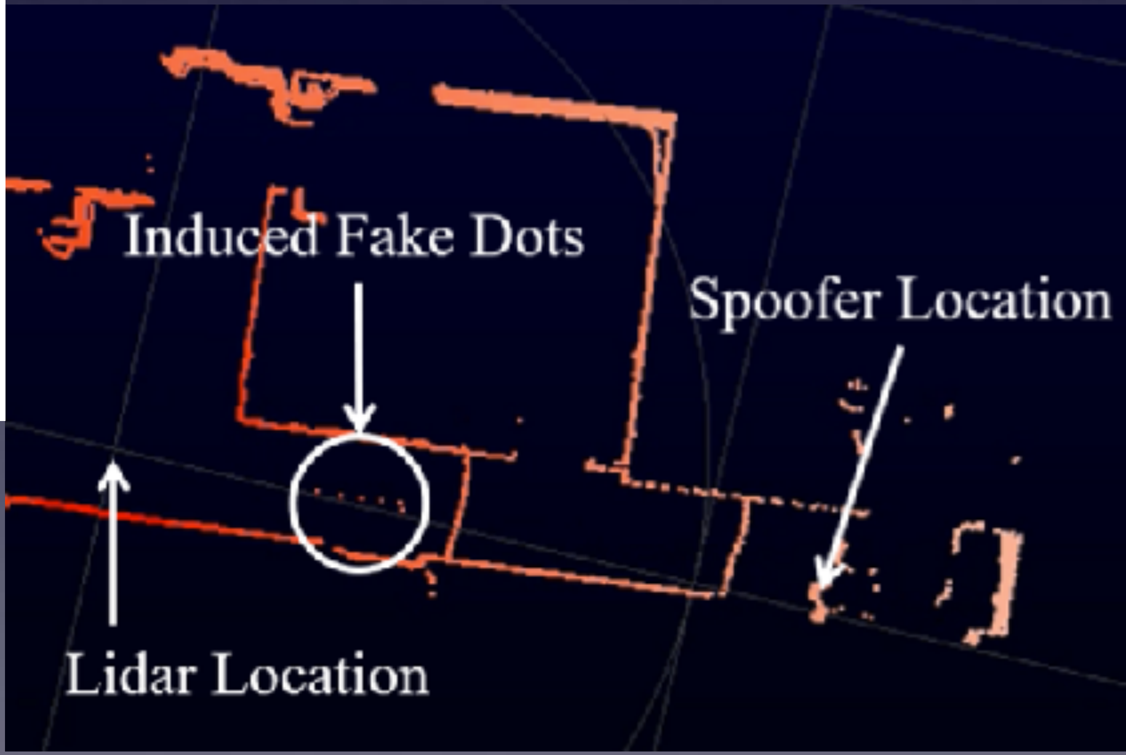
- Spoofing: weaker sources cause false returns
  - Can exploit curved glass refraction to alter location of false returns
  - Depends on source strength

LIDAR


① Multiple pulses received due to divergence
PRT (T)
Receiver
Delay Component
Diverging laser beams
Time difference due to position difference
S
Lidar
Transmitter
d_a
S
T
$d_i + d_p$
② Attacking laser pulse fire
Intensity
Lidar receiving angle aligned toward the transmitter
①
②
Time

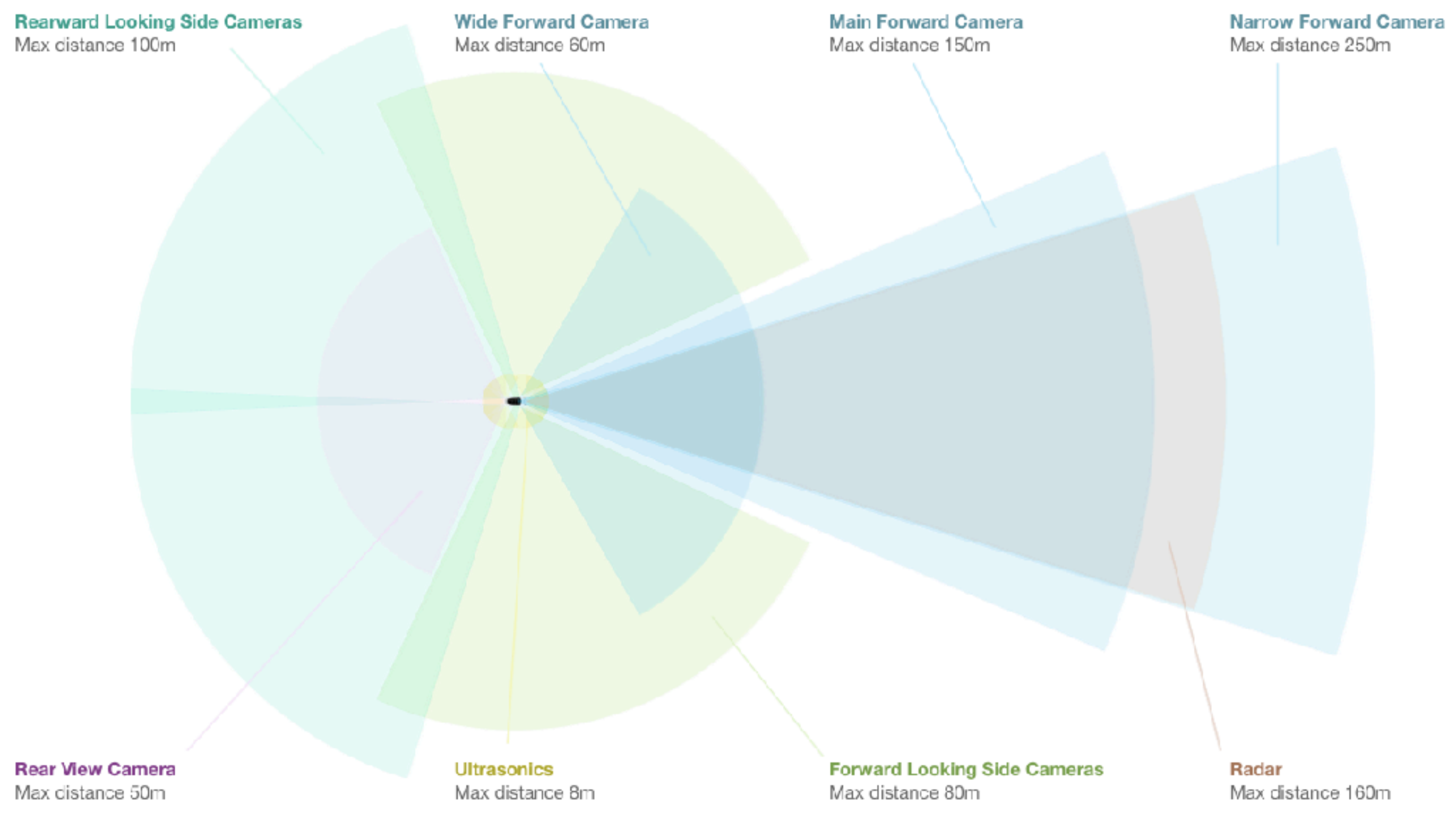
Shin, Kim, Kwon, Kim, KAIST, 2017



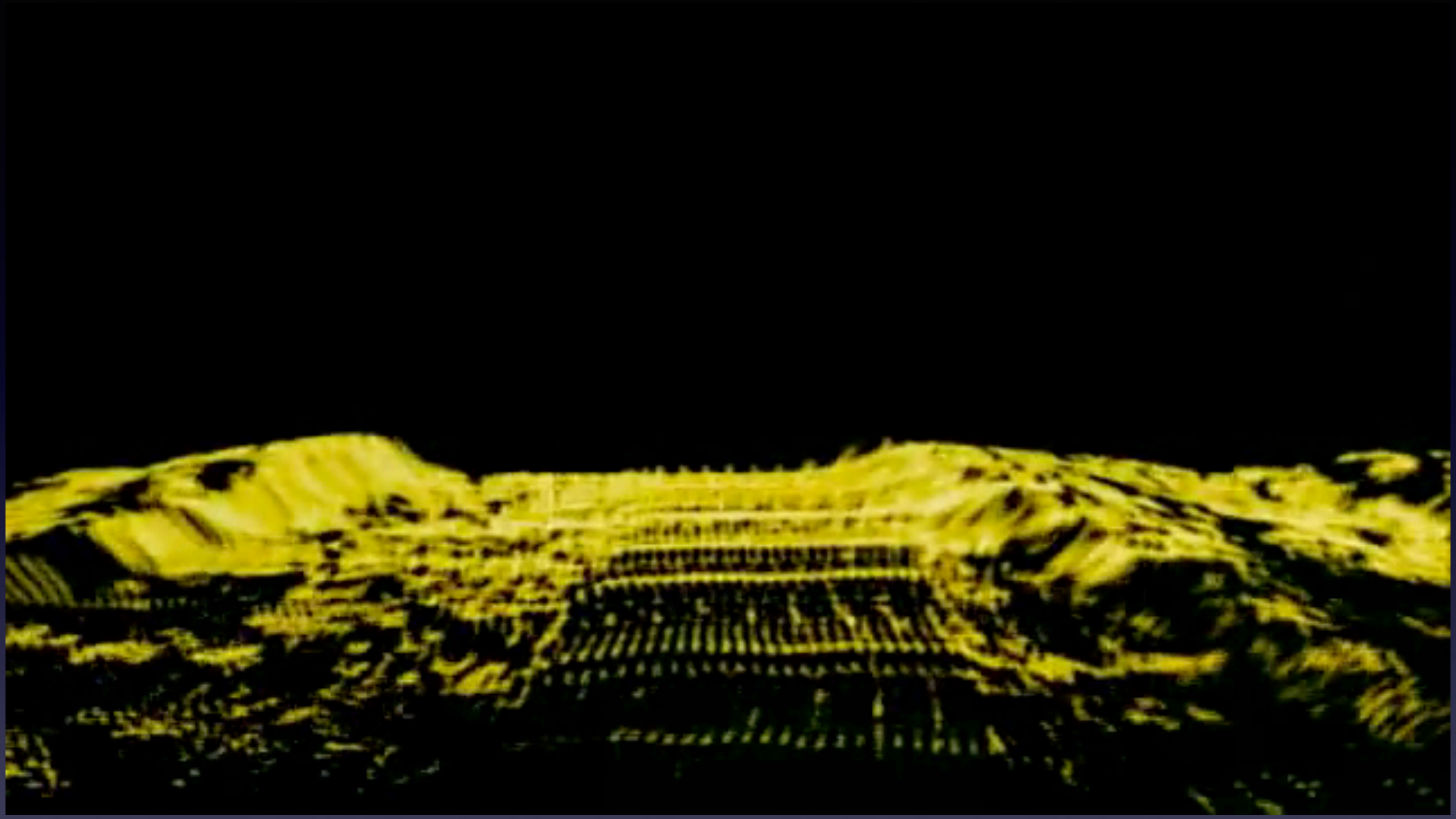


- Spoofing: Relay attack
  - Timing is critical for placement of fake returns

Tesla Autopilot

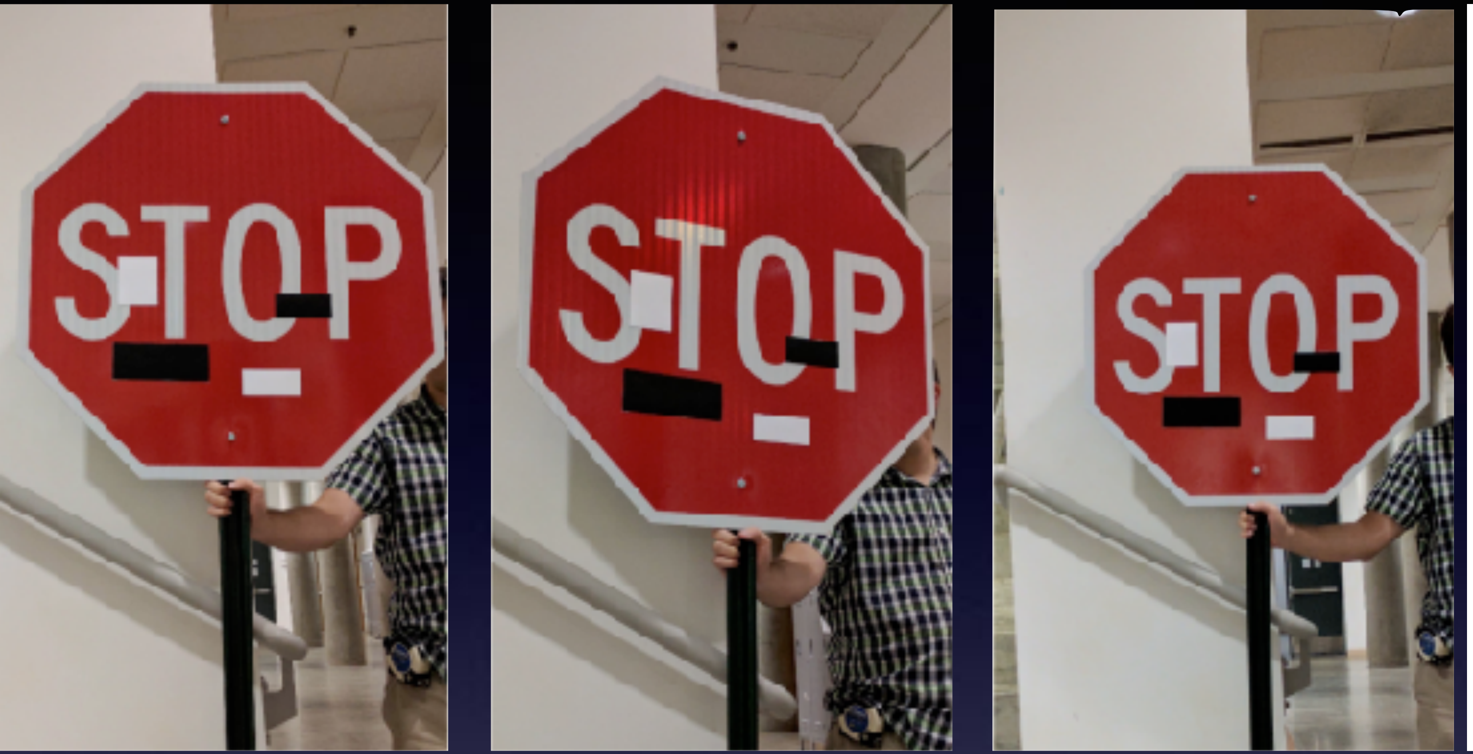


Cameras

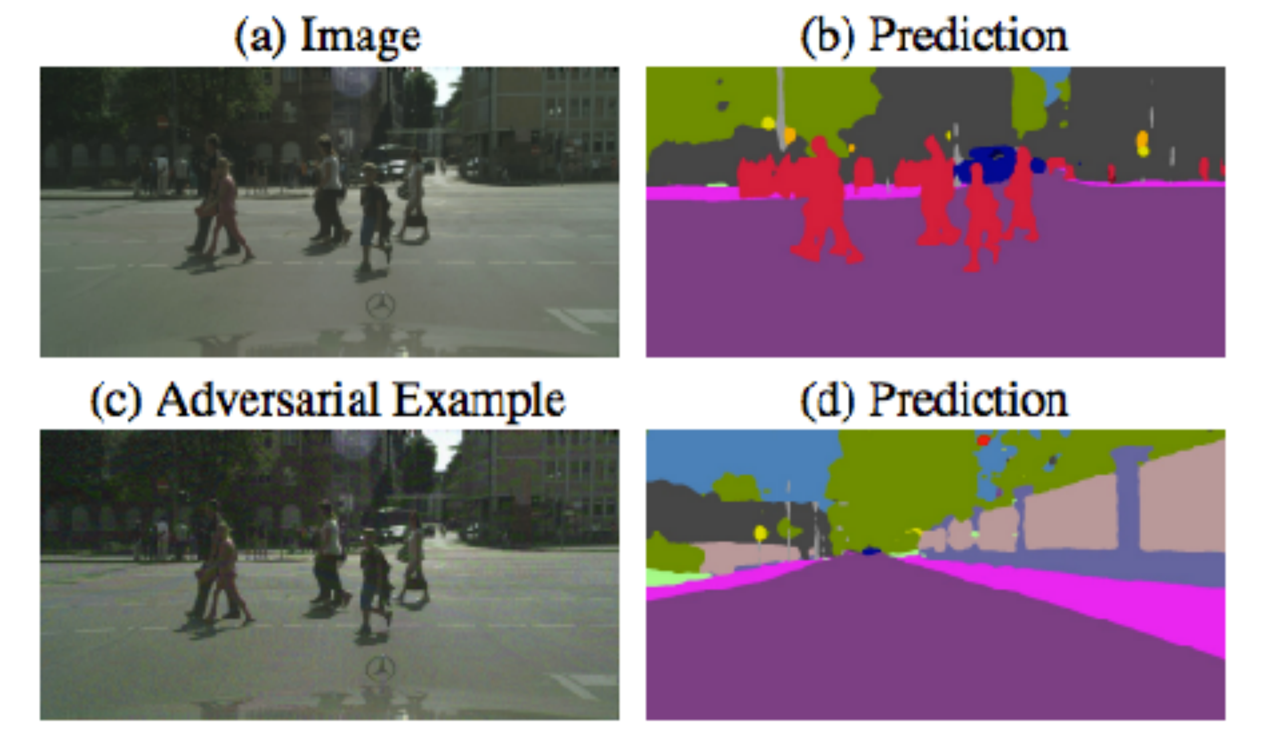


- Specialized object detection
- Sometimes stereo for (noisy!) depth map
- Colorizing LIDAR
- Denial:
  - Easily dazzled
- Spoofing:
  - Camouflage techniques
  - Color assumptions
  - Repeating patterns

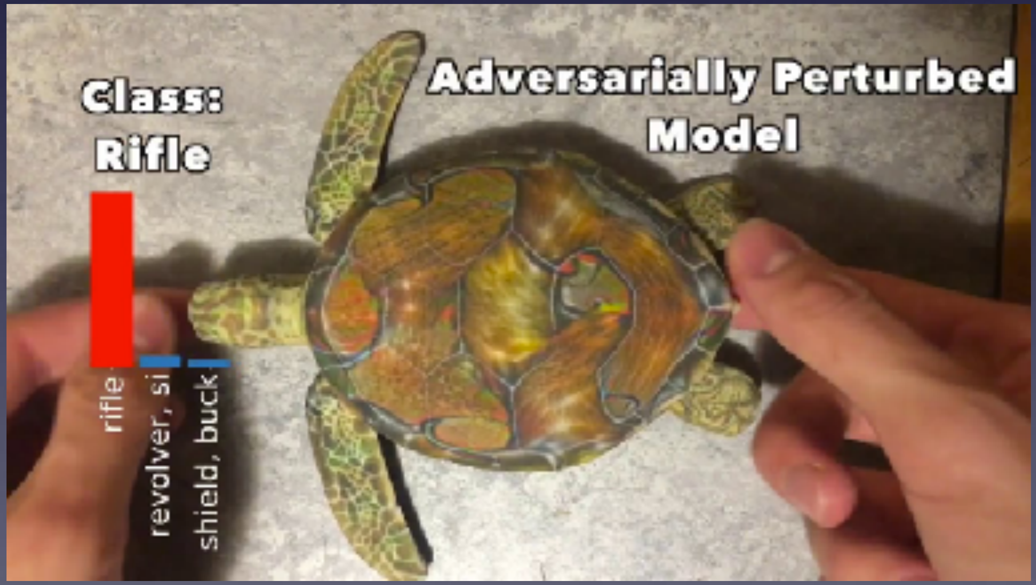
Cameras



Eykholt et al., 2018



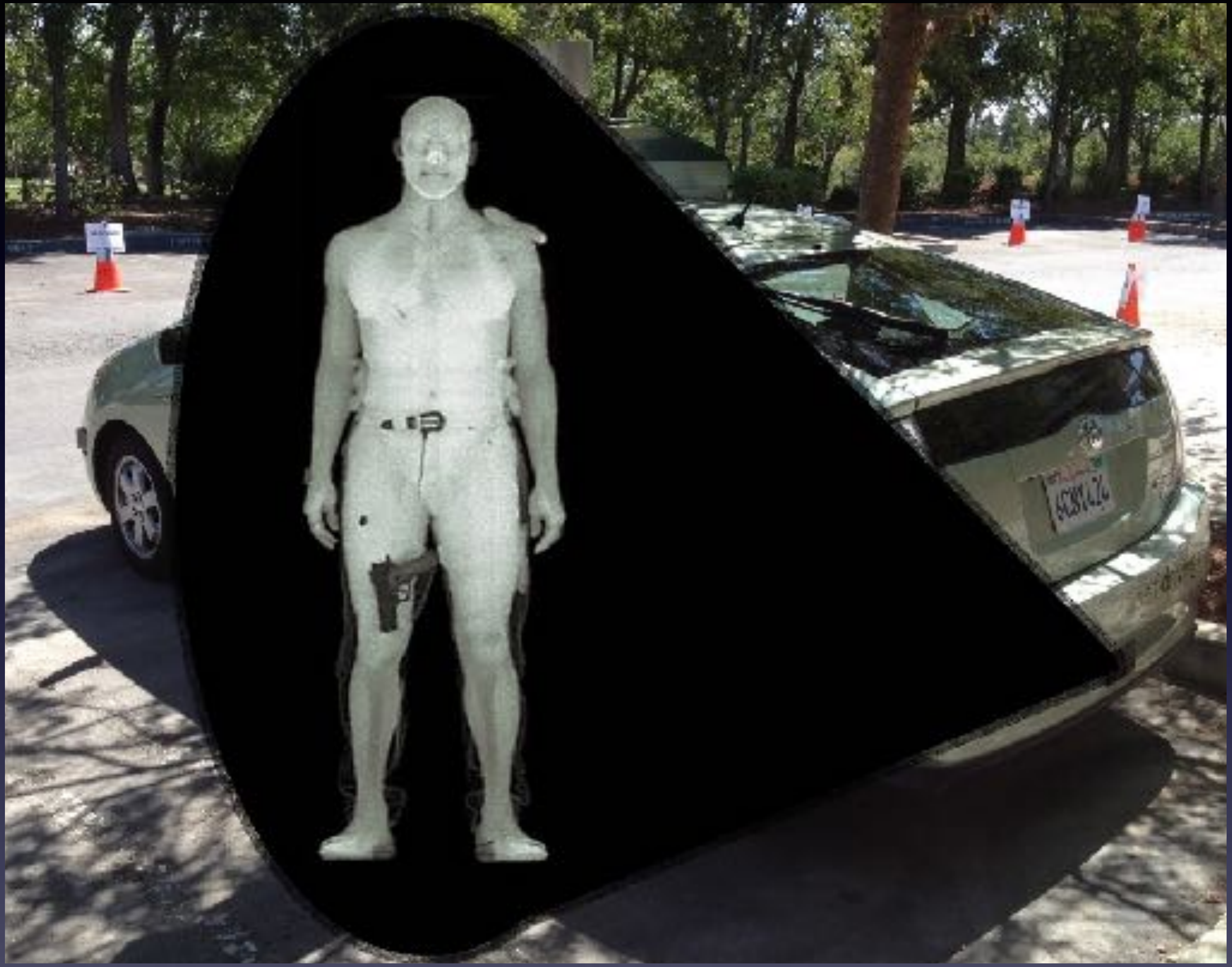
Fischer et al., 2017



Athalye et al., 2018

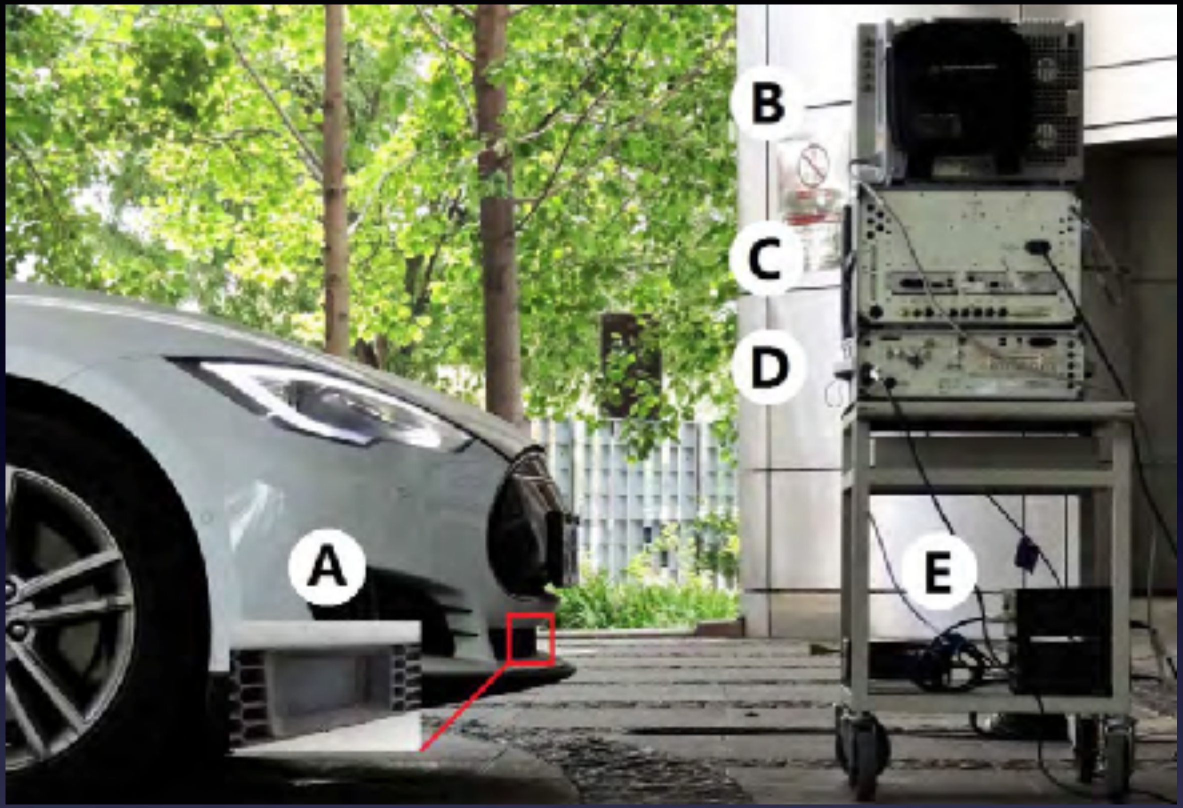
- Spoofing deep learning recognition models
  - Crafted adversarial examples
  - So far generally white box techniques
  - Do not currently work reliably in face of parametric distortions

MMW RADAR



- Collision avoidance
- Lower resolution than laser
- Most things very reflective
- Denial/spoofing:
  - Jamming
  - Chaff
  - Overhead signs

MMW RADAR

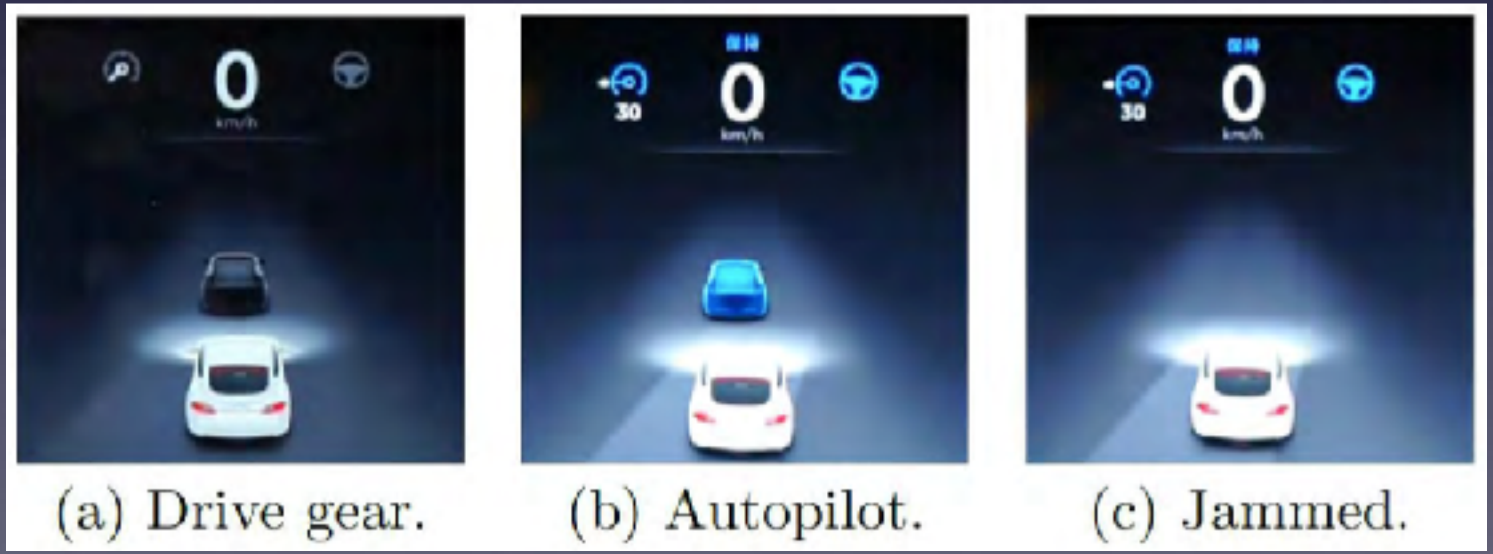


Oscilloscope

Signal Analyzer

Signal Generator

Harmonic Mixer
Frequency Multiplier



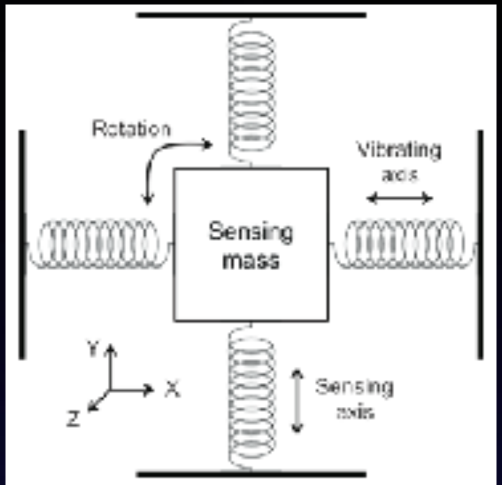
(a) Drive gear. (b) Autopilot. (c) Jammed.

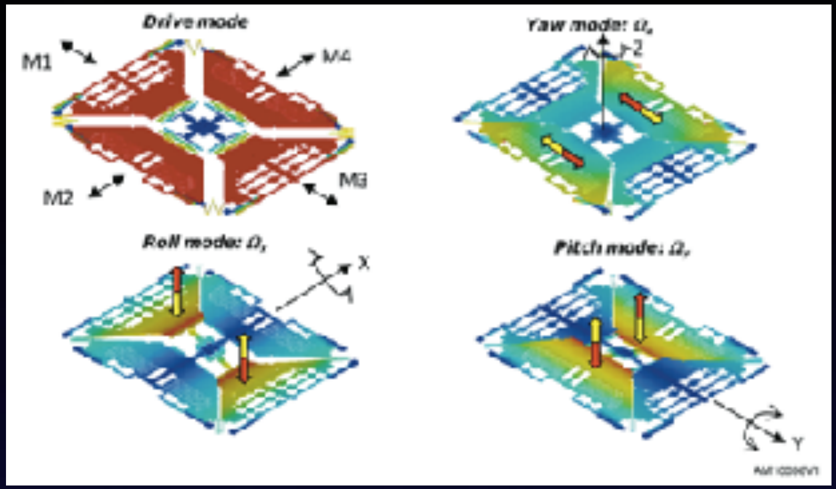
- Jamming: Contactless Sensor Attacks
    - Liu, Yan, Xu, DEF CON 24
    - Spoofing & relay attacks theorized but not performed

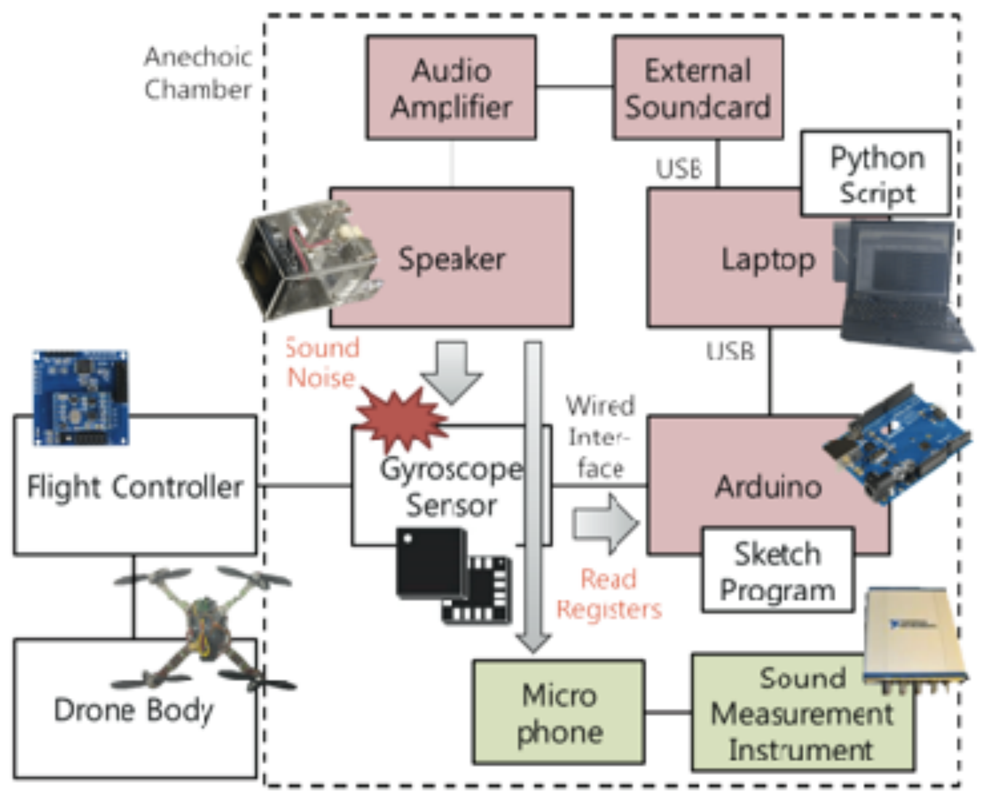
IMU & Compass

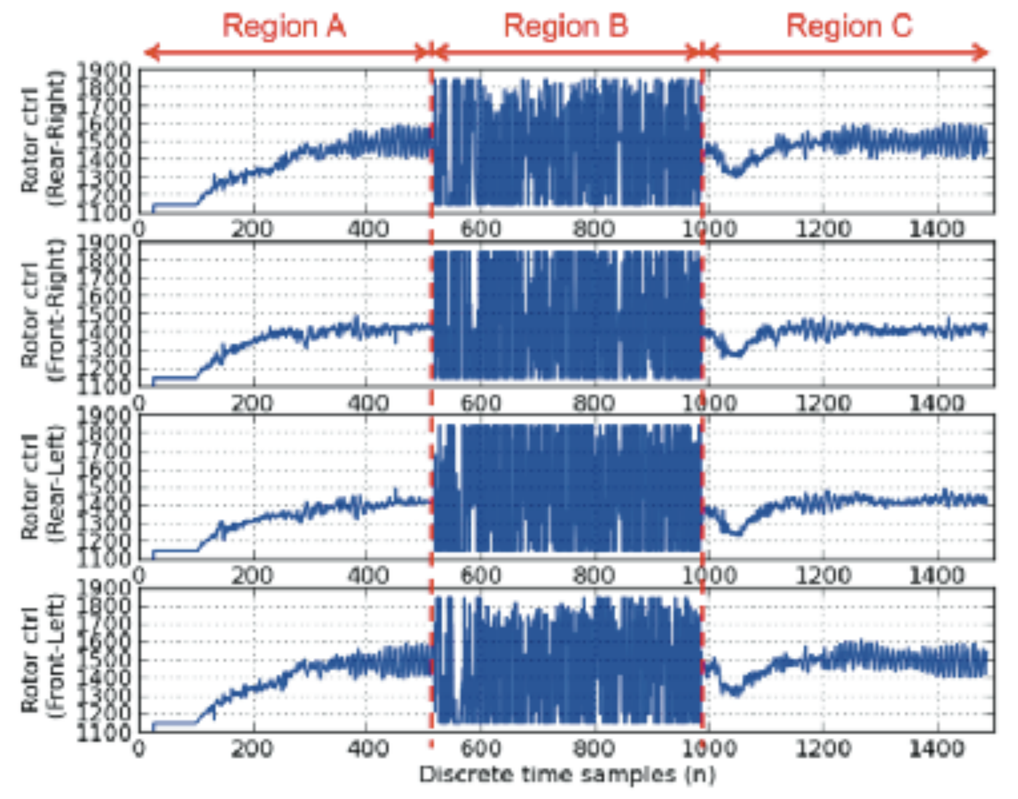
- Primary navigation sensor for some systems
- High fidelity models available
  - Typical cumulative error: 0.1% of distance traveled
- Denial/spoofing:
  - Extremely difficult to interfere with
  - Physical attacks with magnetic fields, thermal drift

IMU Acoustic Attacks





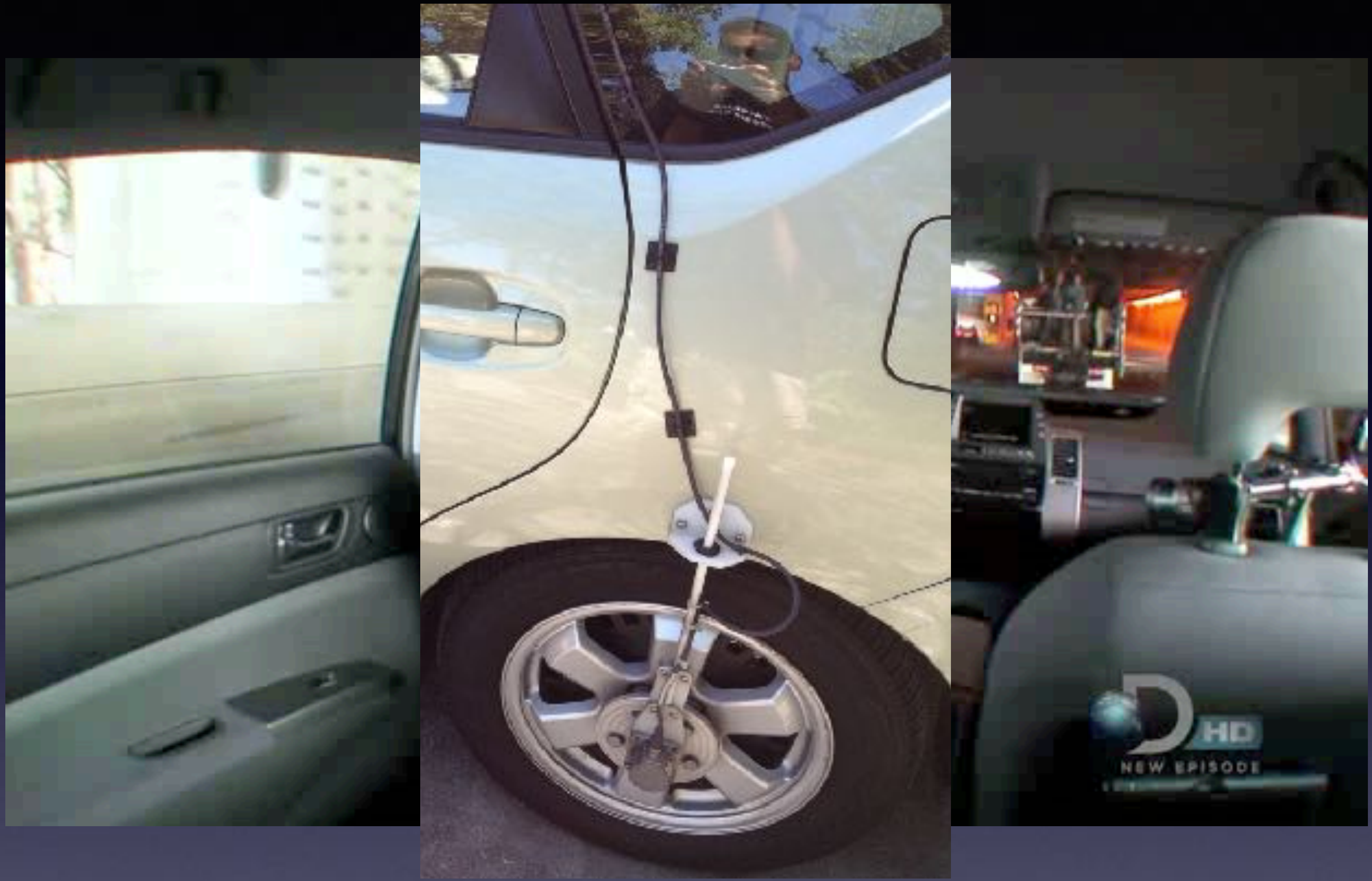




Son et al., KAIST, 2015

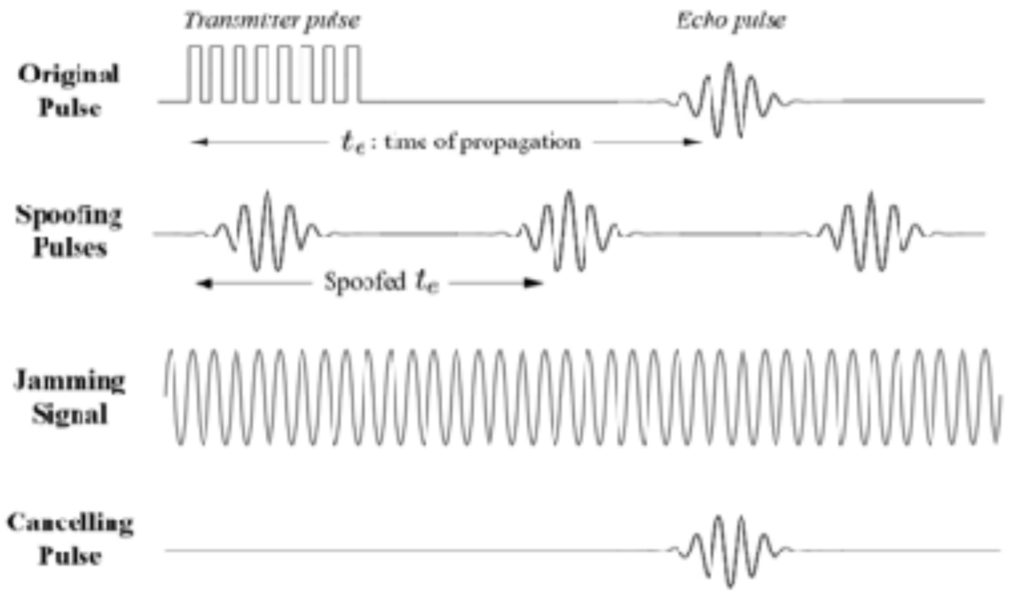
- MEMS gyroscope vibrates & has resonant frequency
  - Can be perturbed with external acoustic source
    - Similar to well-known attacks on spinning hard disks
  - Successfully POC’d by crashing flying multirotor UAV

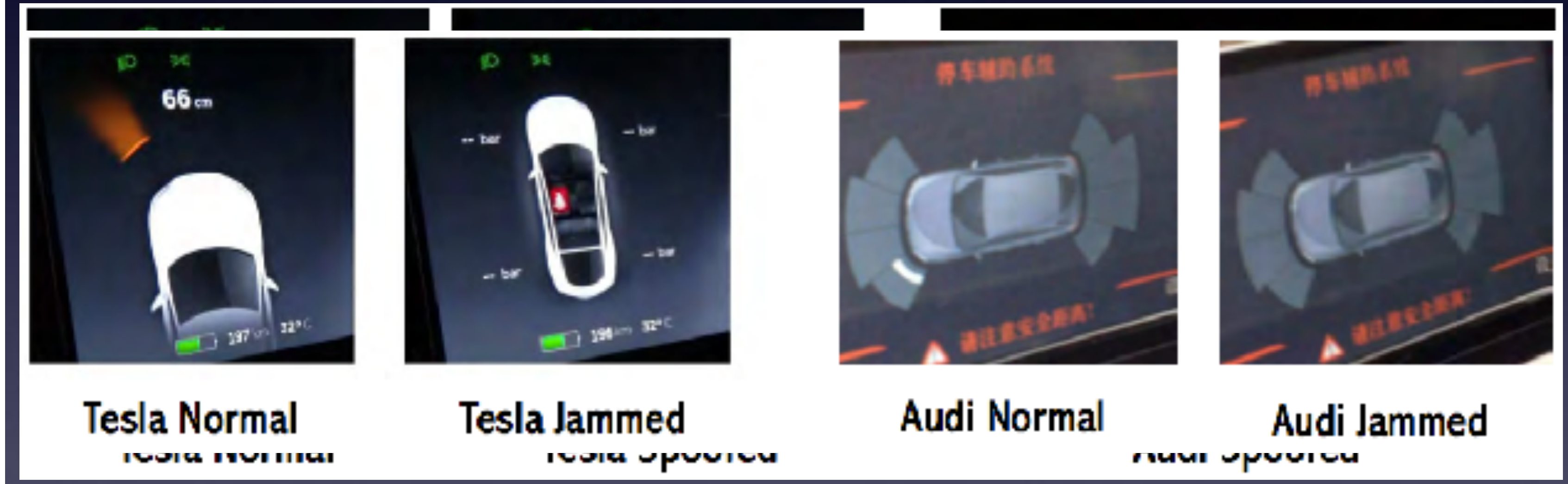
Wheel Odometry



- Encoders
- Useful to know true speed & when stopped
- Attacks:
    - Change wheel diameter
    - Slippery surface
    - Removal may cause unpredictable behavior or stoppage

Ultrasonic Sensors





Contactless Sensor Attacks (Liu, Yan, Xu, DEF CON 24)

- Automated parking sensor
- Only used at low speed
- Attacks:
  - Jamming
  - Spoofing
  - Cancellation

Bond vs Robots

- GPS Jammer
- Smoke/Dust/Vapor
- Lightweight decoy obstacles
- Chaff
- Glass caltrops
- Oil slick

Bond vs Robots

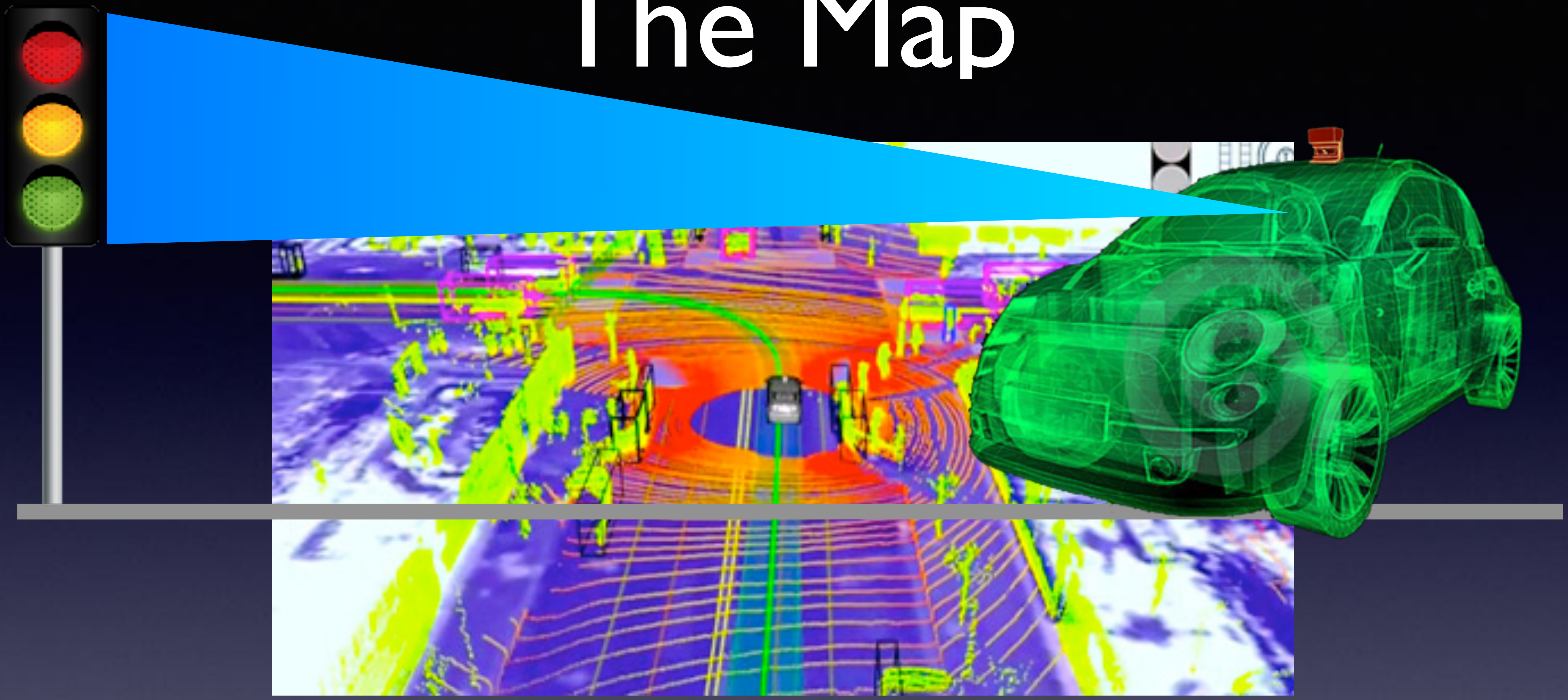
- Active LIDAR Jammer/Spoofer
- Active Radar Jammer
- Acoustic Blaster
- Adversarial Turtle Dispenser

The Map

HD
NEW EPISODE

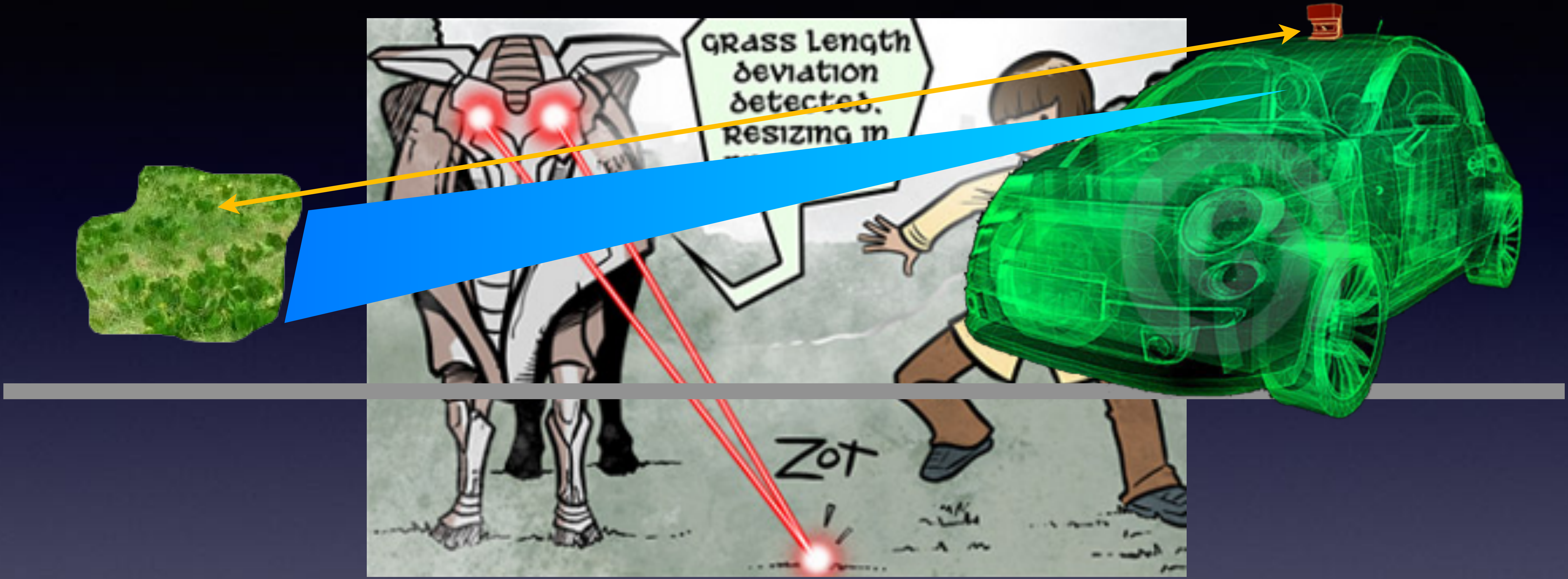
- Great emphasis on preacquired map data
- Often considered to be reference ground truth
- Reduces recognition load
    - Traffic lights
    - Vegetation
    - Other speed control & traffic management features

The Map



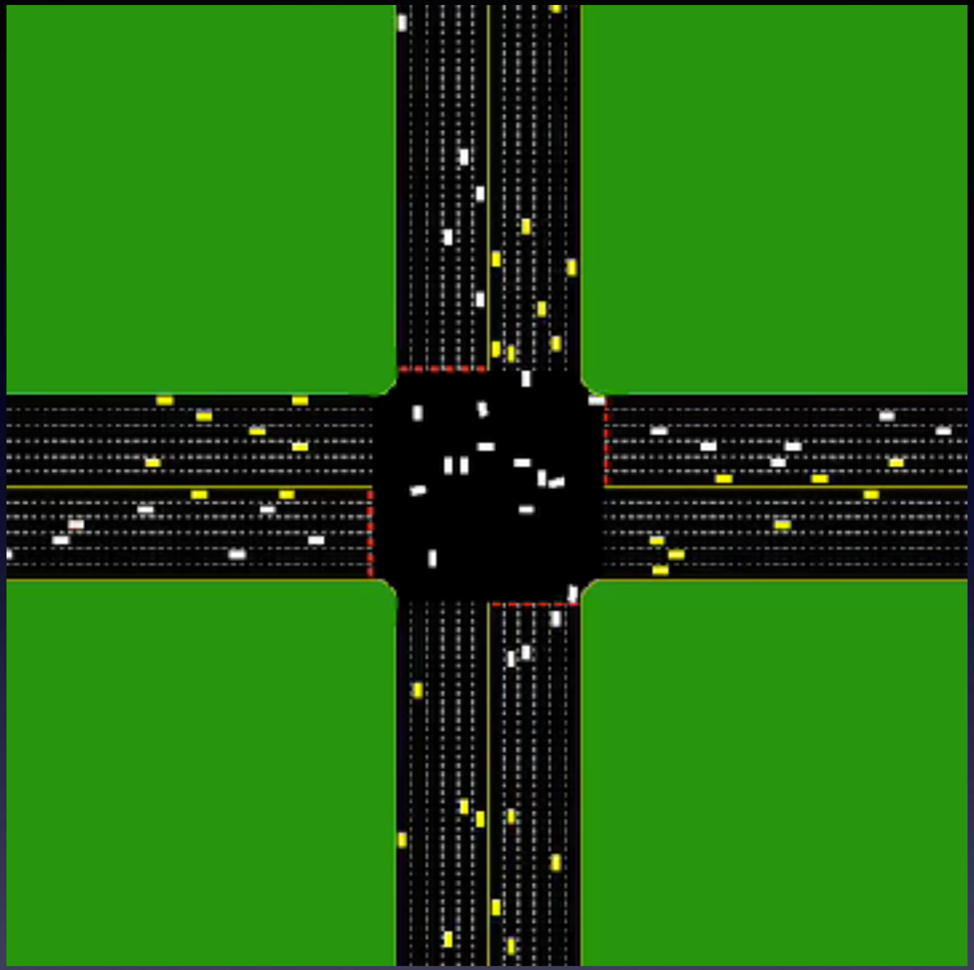
- Traffic lights
  - Camera knows where to look
  - Difference in robot vs human assumptions

The Map



- Vegetation
  - Colorized LIDAR
  - Transmission classifier
- Overhanging foliage
- Map dependence may exacerbate brittleness of discrimination rules

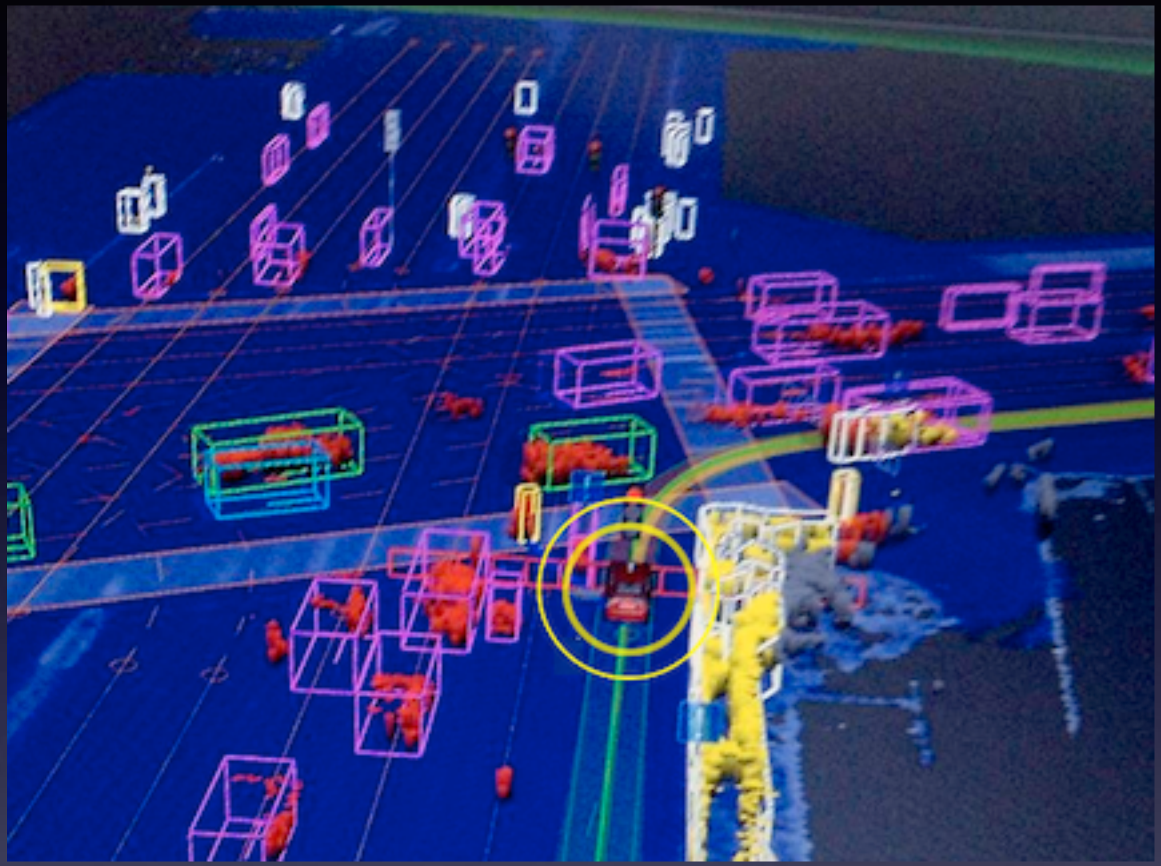
The Map



Peter Stone, UT Austin

- Map requires constant updates
- Local map:
  - Vulnerable to unexpected real world features
- Remote map:
  - Vulnerable to denial (4G jamming)
  - Vulnerable to spoofing (MITM attack, standard cellular intercept techniques)

Exploiting the Logic Structure

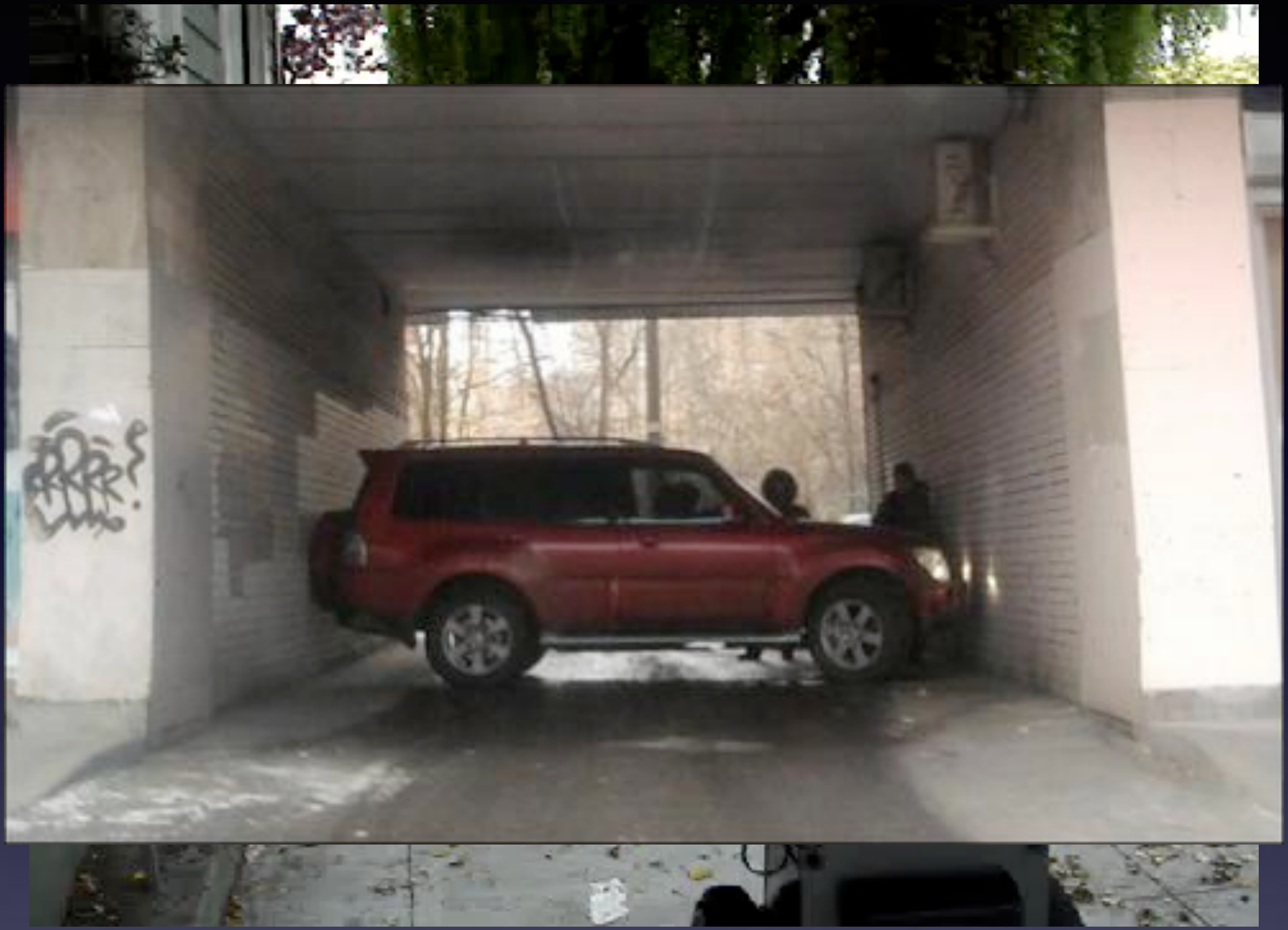


- Goal: Maximize uncertainty
  - Requiring manual assistance
  - Confusing/annoying occupants
  - Inconveniencing other road users
- Concentrate on fragile maneuvers

Logic-Based Physical Attacks

- 21st century sabotage
- Dependent on vehicle configuration & mission
- 4G, GPS-enabled electromagnet/heating unit
  - Near IMU/compass/MMW
- Triggered by map location/activity

Trapping/Redirecting



- Attacks at collision avoidance & navigation layers
- Force robot to postpone high level tasks
  - Moving obstacles
  - Obstacle swarms
  - Artificial stop signs
- Human driver wouldn’t notice, robot can’t ignore

Clobbering

- Goal: make robot run into something
- Subvert collision avoidance
    - Incapacitate vehicle
    - Damage/remove sensors
- Subtle map deviations
- Imitate light vegetation
- Simulate obstacles at speed
- Disguise entrance walls with reflective/absorbent material within GPS noise
- Dynamic obstacles under overhead signs

Remember...

Driverless vehicles are cool!

Don’t do any of these things!

~~Don’t hassle the Hoff!~~

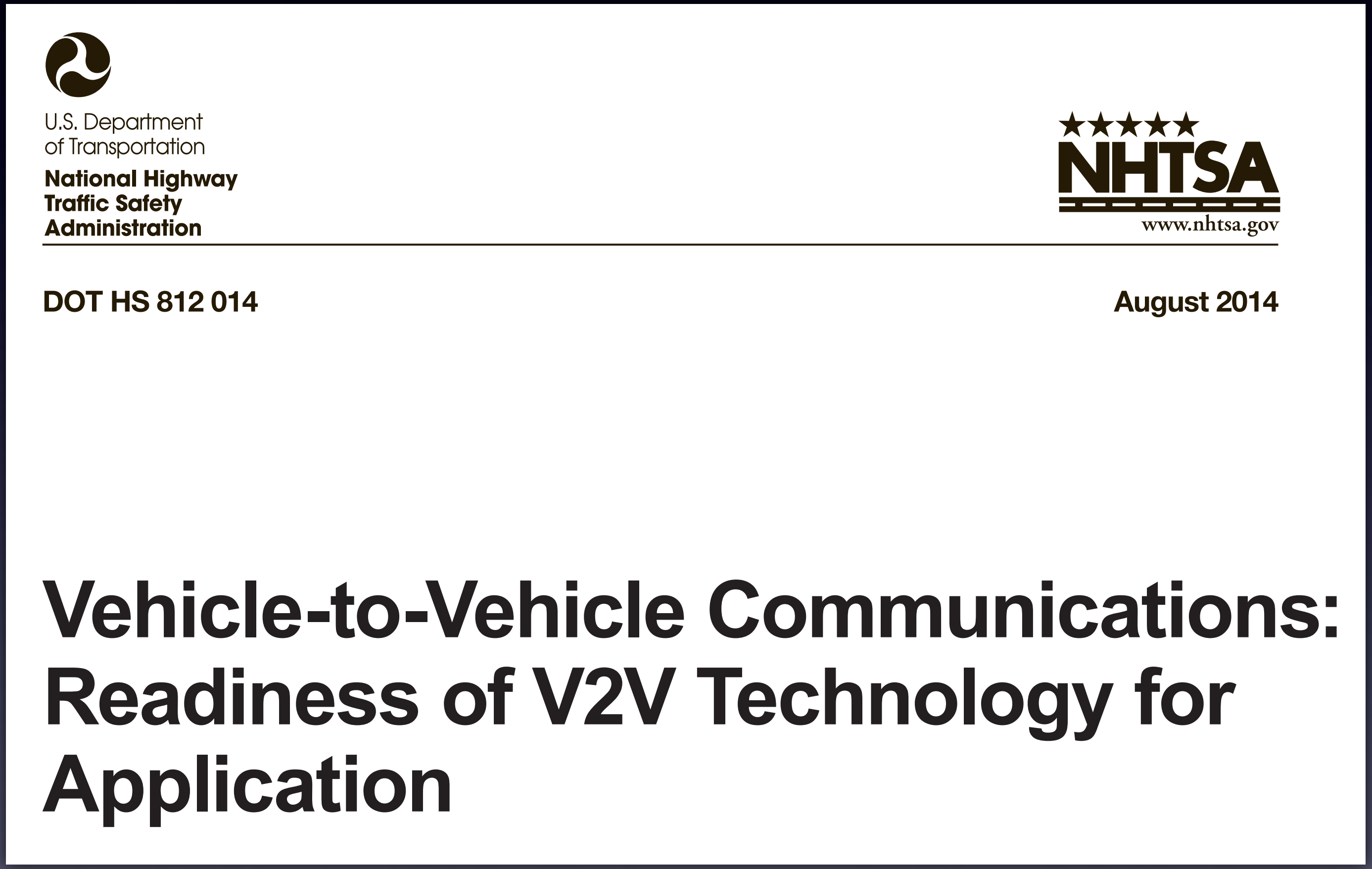
Don’t hax0r the Bots!

Would you buy a self-driving car that couldn’t drive itself in 99 percent of the country? Or that knew nearly nothing about parking, couldn’t be taken out in snow or heavy rain, and would drive straight over a gaping pothole?

If your answer is yes, then check out the Google Self-Driving Car, model year 2014.

— *MIT Technology Review, August 2014*

V2V



U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

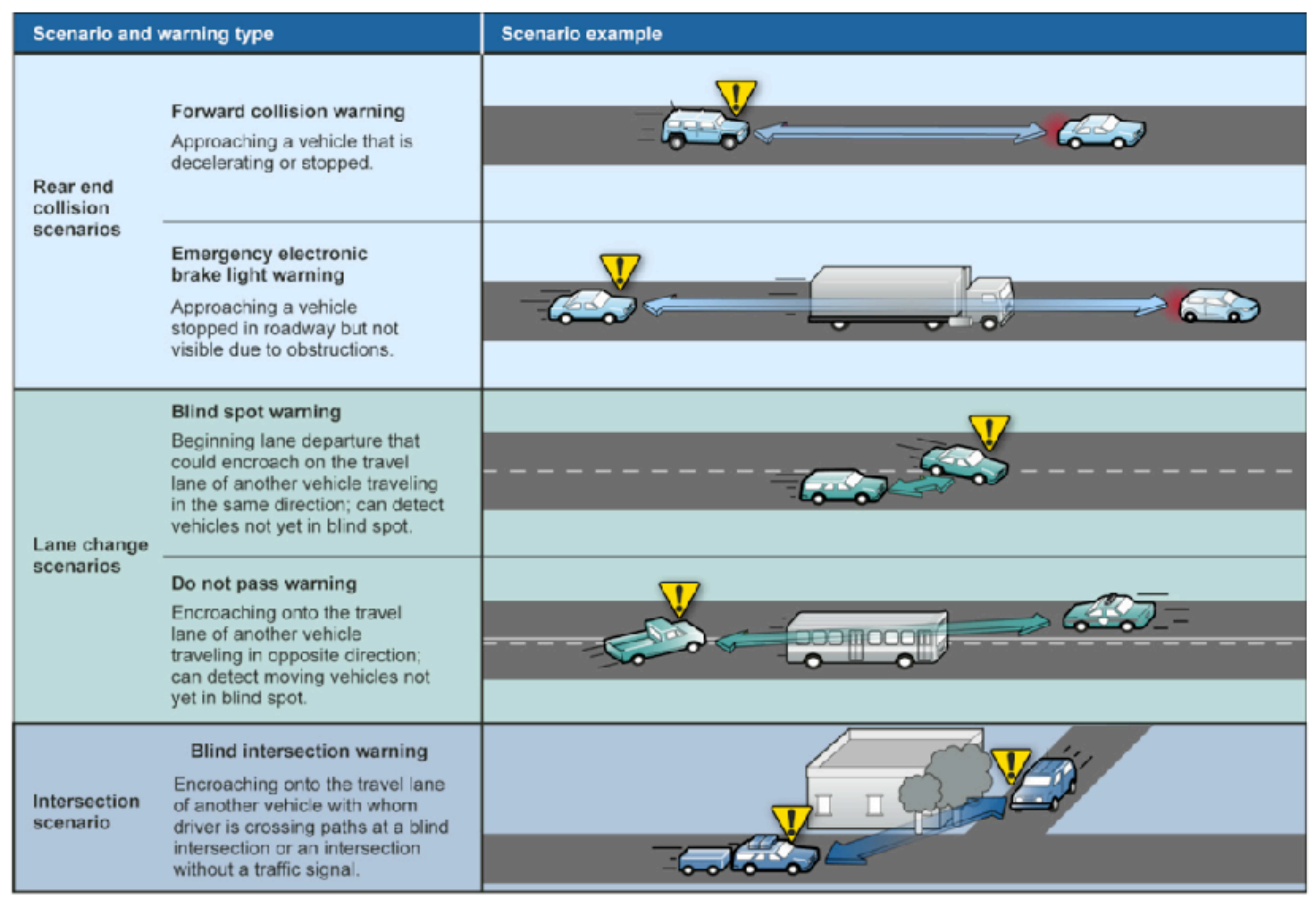
★★★★★
NHTSA
www.nhtsa.gov

DOT HS 812 014

August 2014

Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application

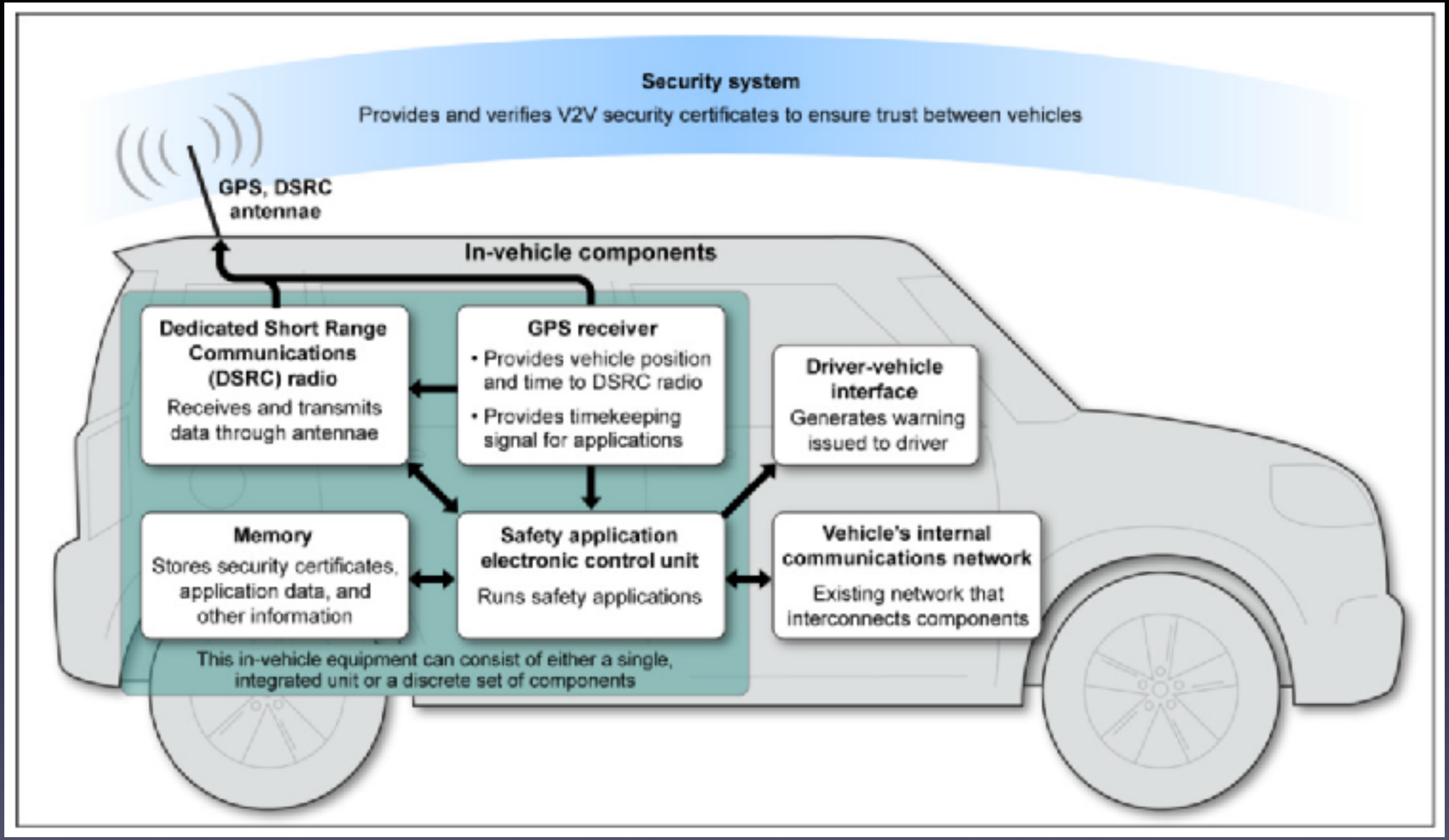
V2V Components



Scenario and warning type		Scenario example
Rear end collision scenarios	**Forward collision warning** Approaching a vehicle that is decelerating or stopped.	
	Emergency electronic brake light warning Approaching a vehicle stopped in roadway but not visible due to obstructions.	
Lane change scenarios	**Blind spot warning** Beginning lane departure that could encroach on the travel lane of another vehicle traveling in the same direction; can detect vehicles not yet in blind spot.	
	Do not pass warning Encroaching onto the travel lane of another vehicle traveling in opposite direction; can detect moving vehicles not yet in blind spot.	
Intersection scenario	**Blind intersection warning** Encroaching onto the travel lane of another vehicle with whom driver is crossing paths at a blind intersection or an intersection without a traffic signal.	

- Just warnings for now!

V2V Components



Security system
Provides and verifies V2V security certificates to ensure trust between vehicles
GPS, DSRC antennae
In-vehicle components
Dedicated Short Range Communications (DSRC) radio
Receives and transmits data through antennae
GPS receiver
• Provides vehicle position and time to DSRC radio
• Provides timekeeping signal for applications
Driver-vehicle interface
Generates warning issued to driver
Memory
Stores security certificates, application data, and other information
Safety application electronic control unit
Runs safety applications
Vehicle's internal communications network
Existing network that interconnects components
This in-vehicle equipment can consist of either a single, integrated unit or a discrete set of components

- Both on-board and roadside communicators
- DSRC: Omnidirectional, 300m range, 200-500 bytes
- Basic Safety Message (BSM) protocol
  - Not encrypted
  - PKI authenticated (signed via certificates)

V2V Transmissions

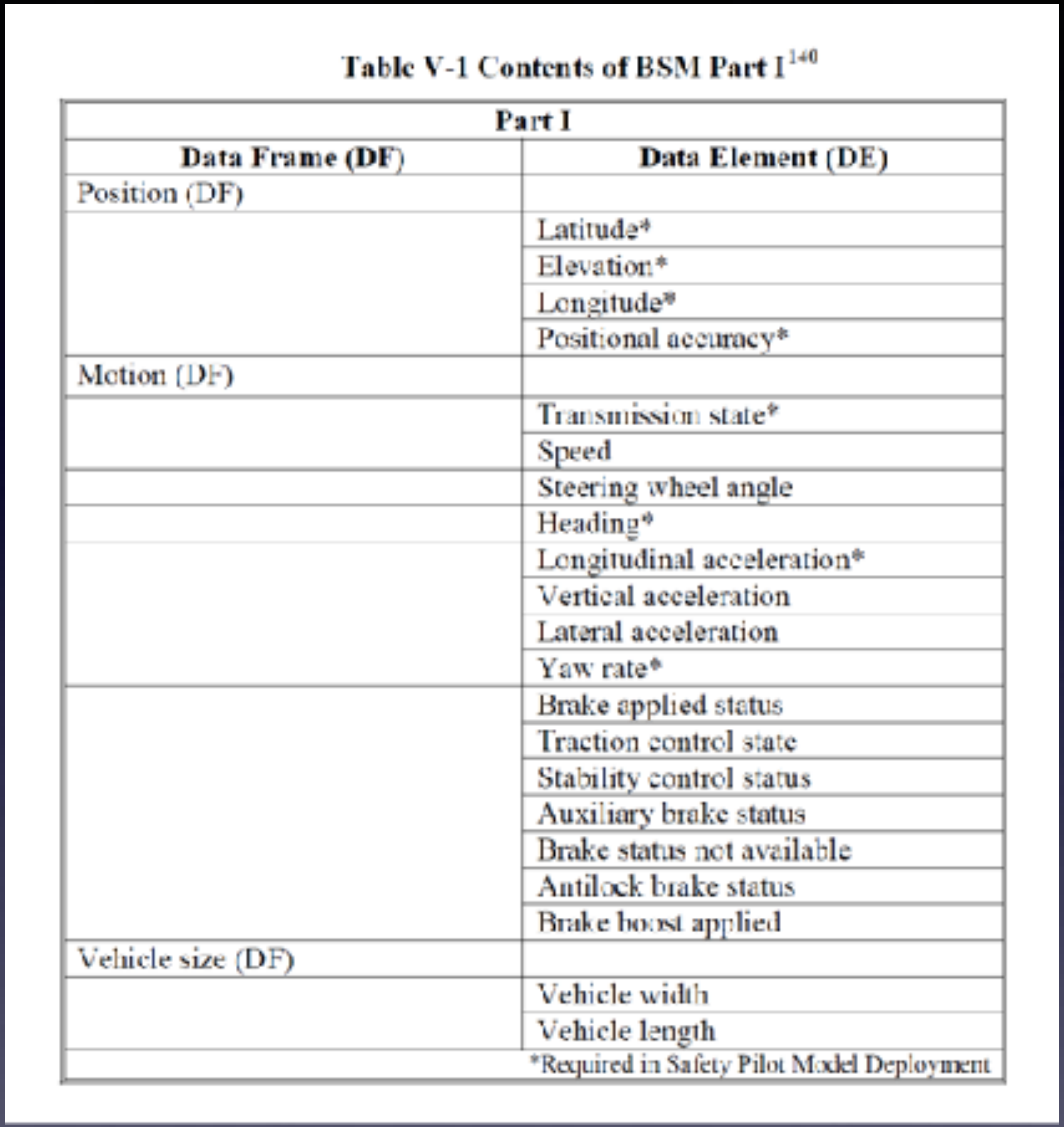
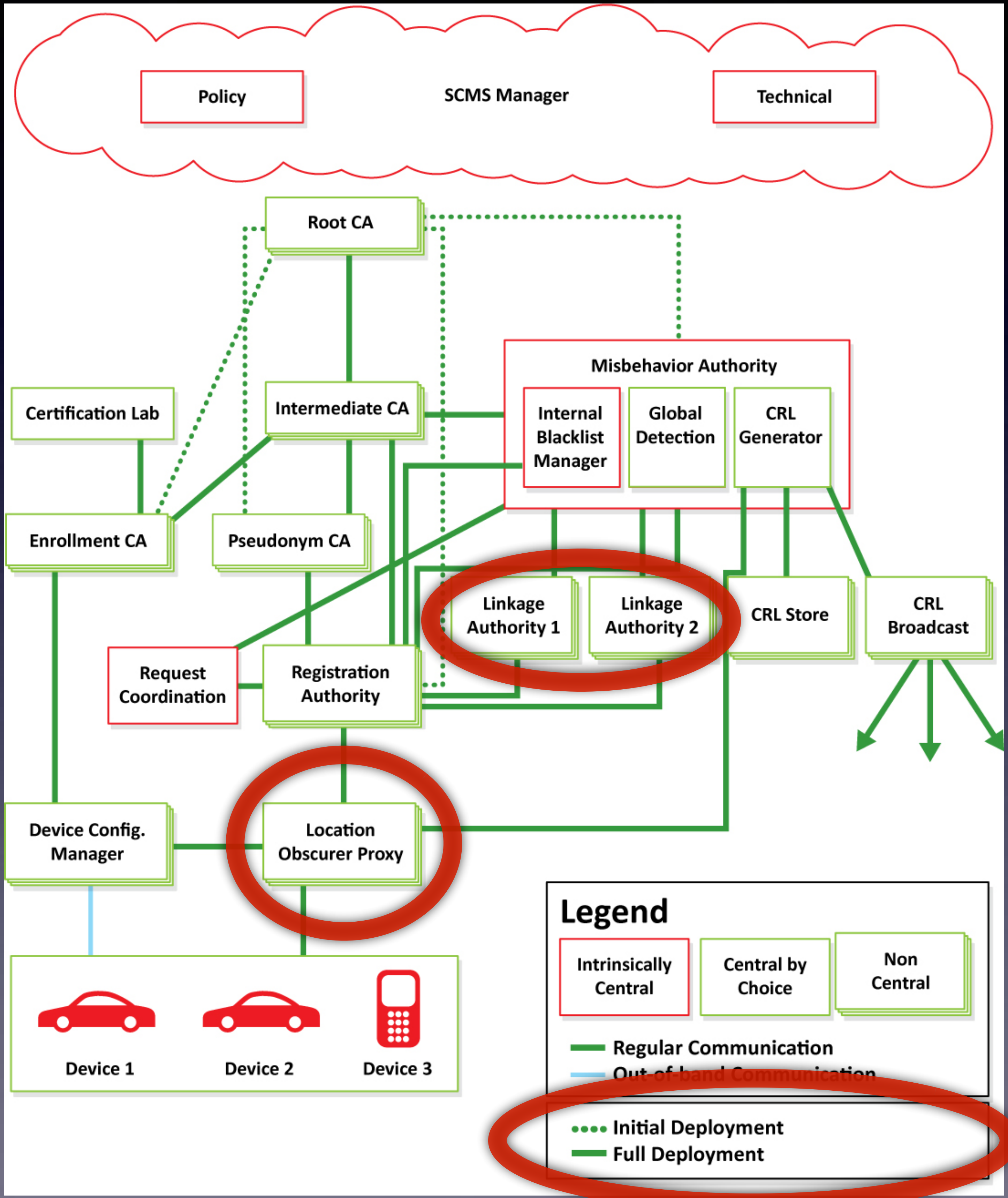


Table V-1 Contents of BSM Part I[140]

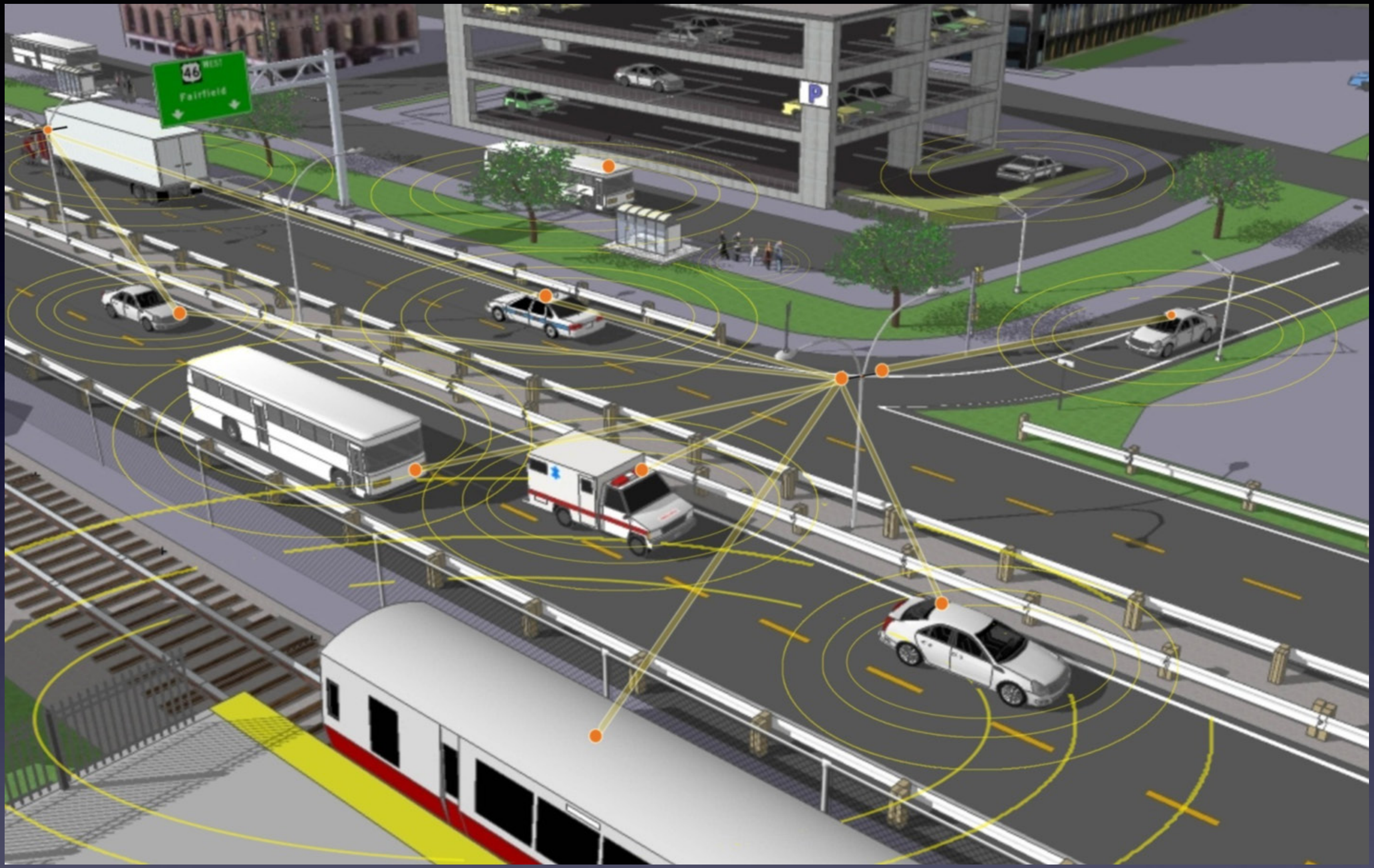
Part I	
Data Frame (DF)	**Data Element (DE)**
Position (DF)	
	Latitude*
	Elevation*
	Longitude*
	Positional accuracy*
Motion (DF)	
	Transmission state*
	Speed
	Steering wheel angle
	Heading*
	Longitudinal acceleration*
	Vertical acceleration
	Lateral acceleration
	Yaw rate*
	Brake applied status
	Traction control state
	Stability control status
	Auxiliary brake status
	Brake status not available
	Antilock brake status
	Brake boost applied
Vehicle size (DF)	
	Vehicle width
	Vehicle length
	*Required in Safety Pilot Model Deployment

- Part I: Core
  - Part II: Appended when changed, vehicle-specific
  - Note unencrypted GPS
    - Spoofing feedback?

V2V Security

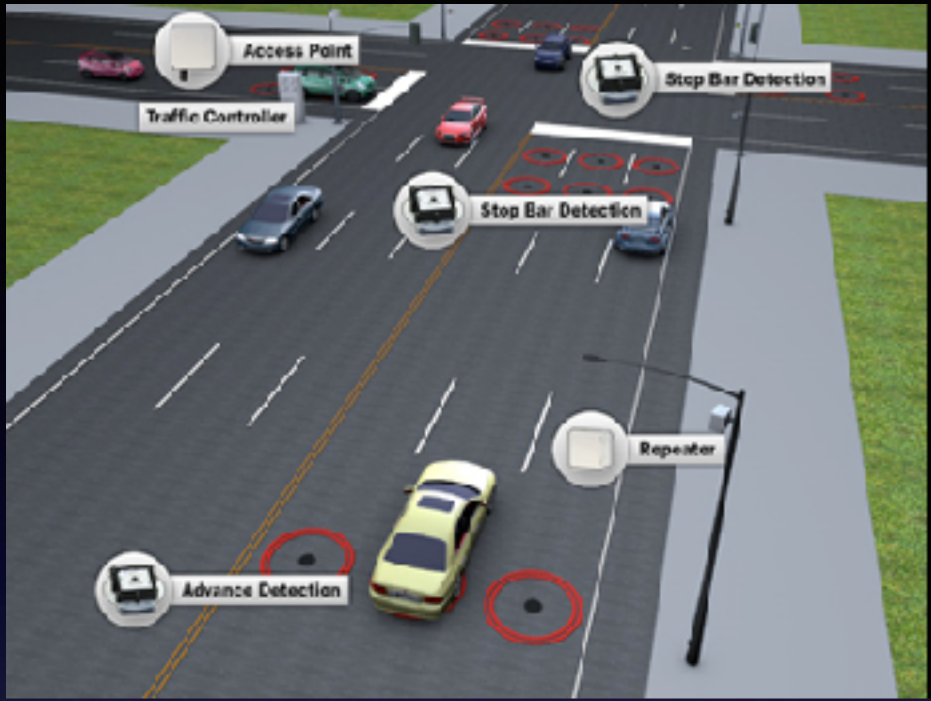


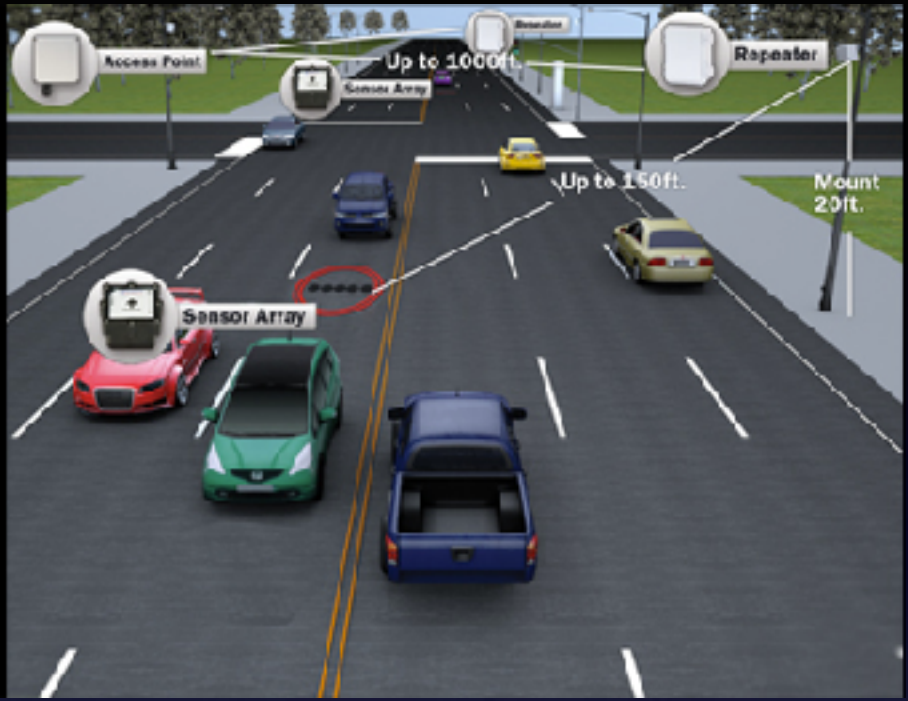
V2V Bottom Lines



- Careful rollout: 11 year development
- Slow & steady rollout: 37 years to full fleet
- Tracking/Privacy more immediate concern than other malicious attacks
- Standard PKI concerns, many yet TBD
- No direct control imminent (robots might get there first)

Traffic Sensor Flaws





- V2V/V2I aims to avoid mistakes of current traffic sensors
  - Hacking US Traffic Control Systems, Cesar Cerrudo @IOActive, DEF CON 22
    - No encryption/authentication, wireless transmission in cleartext
    - Firmware updates neither encrypted nor signed
- No doubt will make others!

Use those Empty Seats
EMPTY
EMPTY
EMPTY
EMPTY

The car drives *itself* while you “SHAG”!