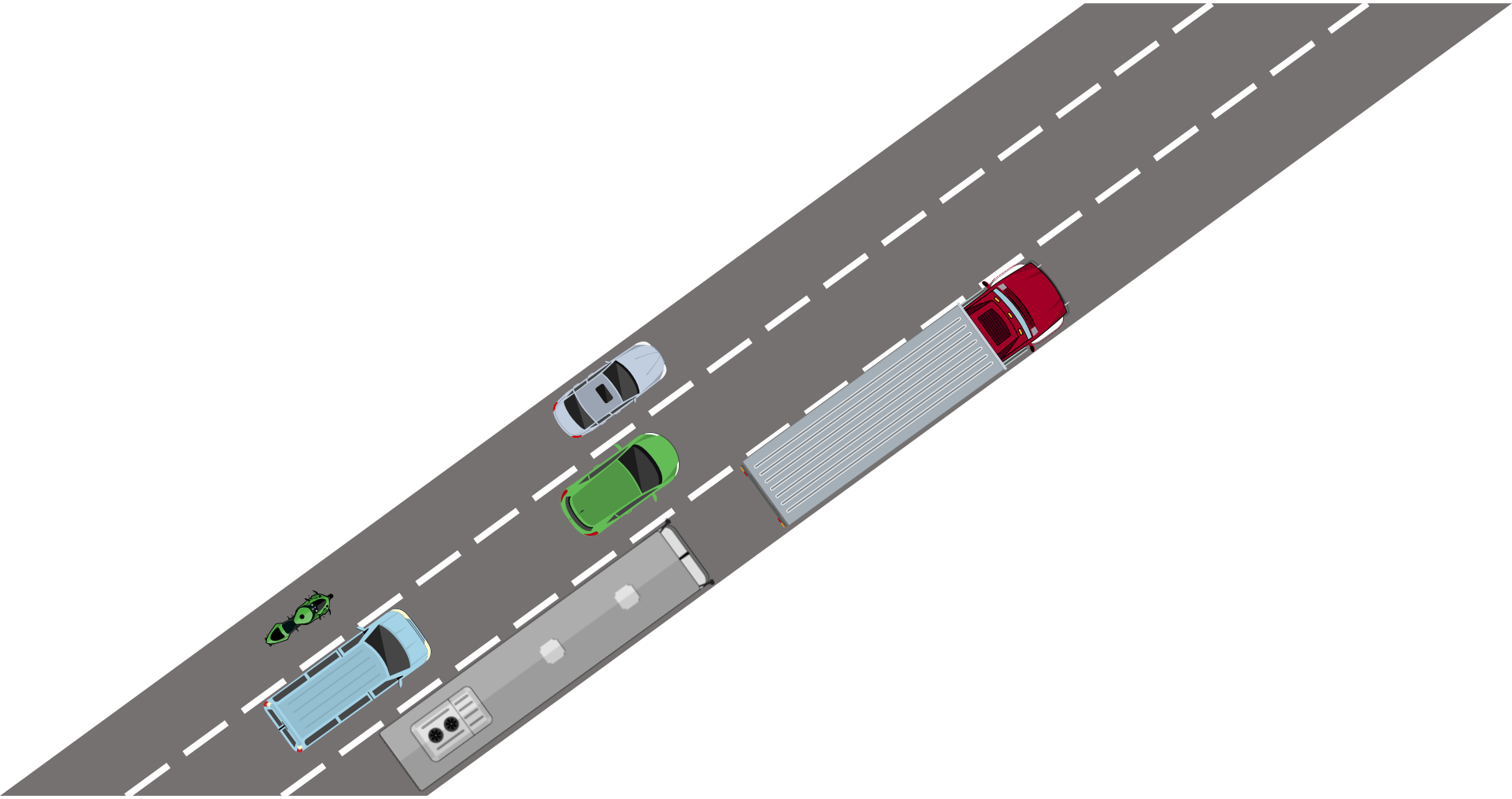
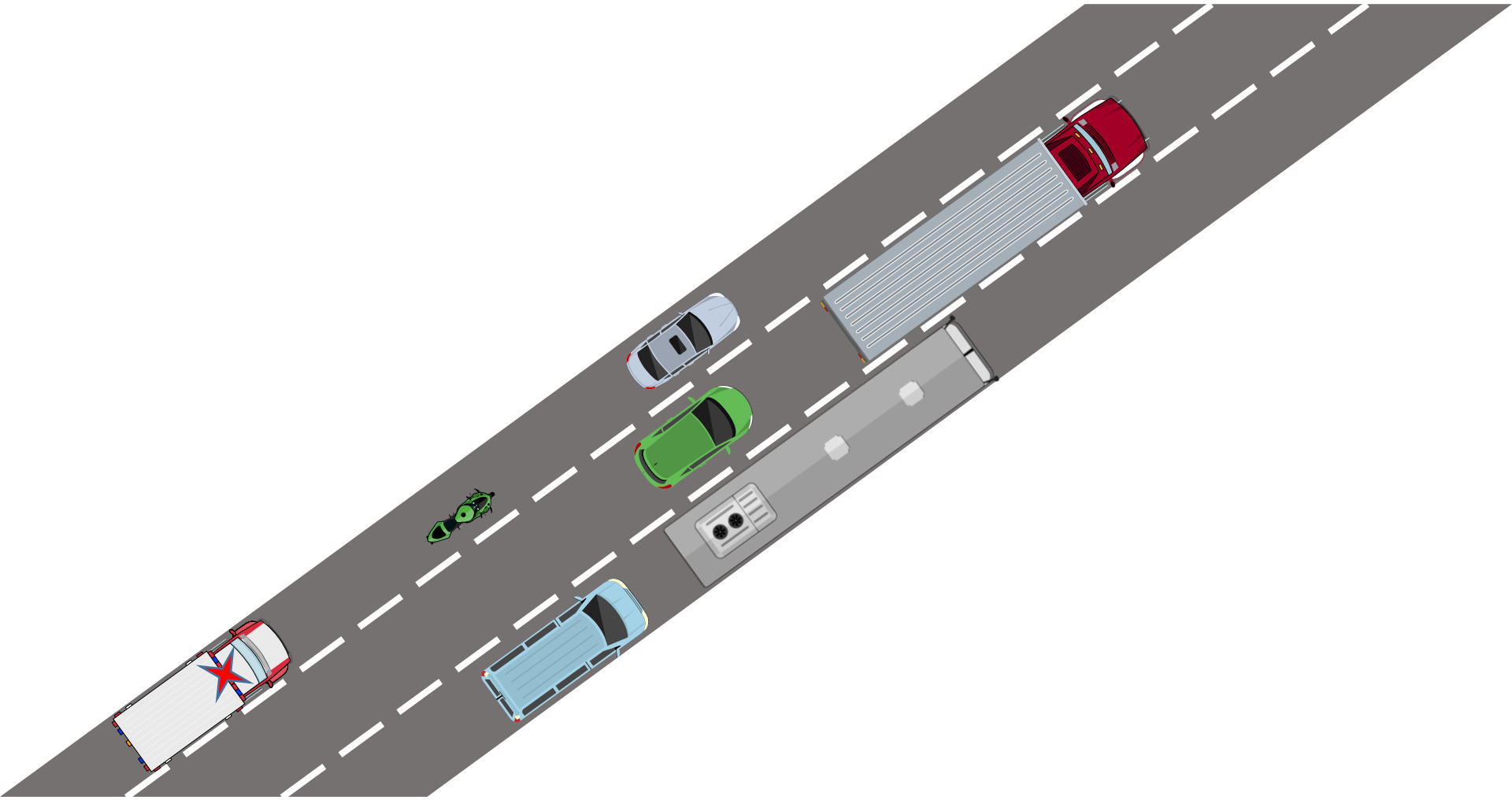
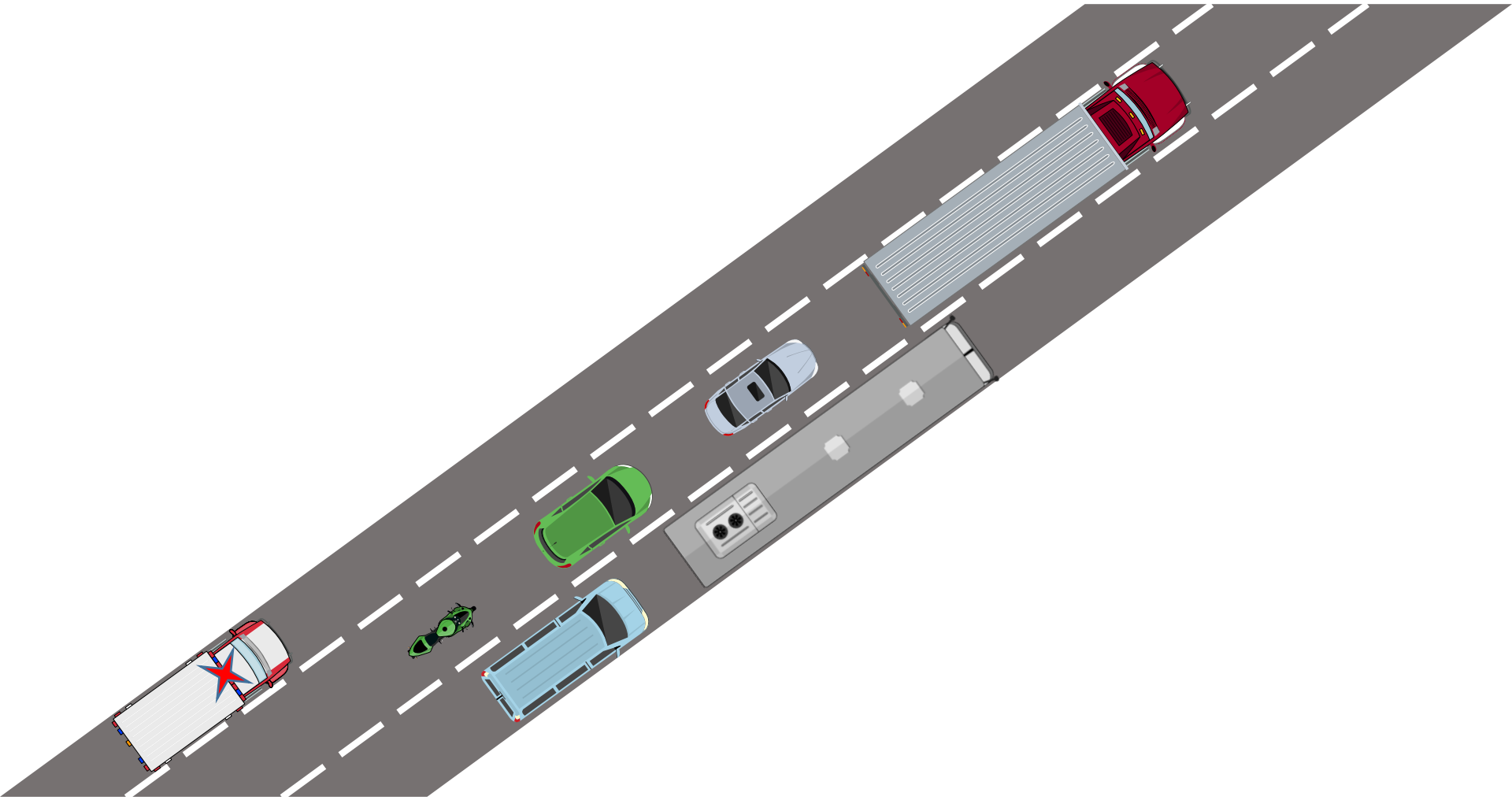
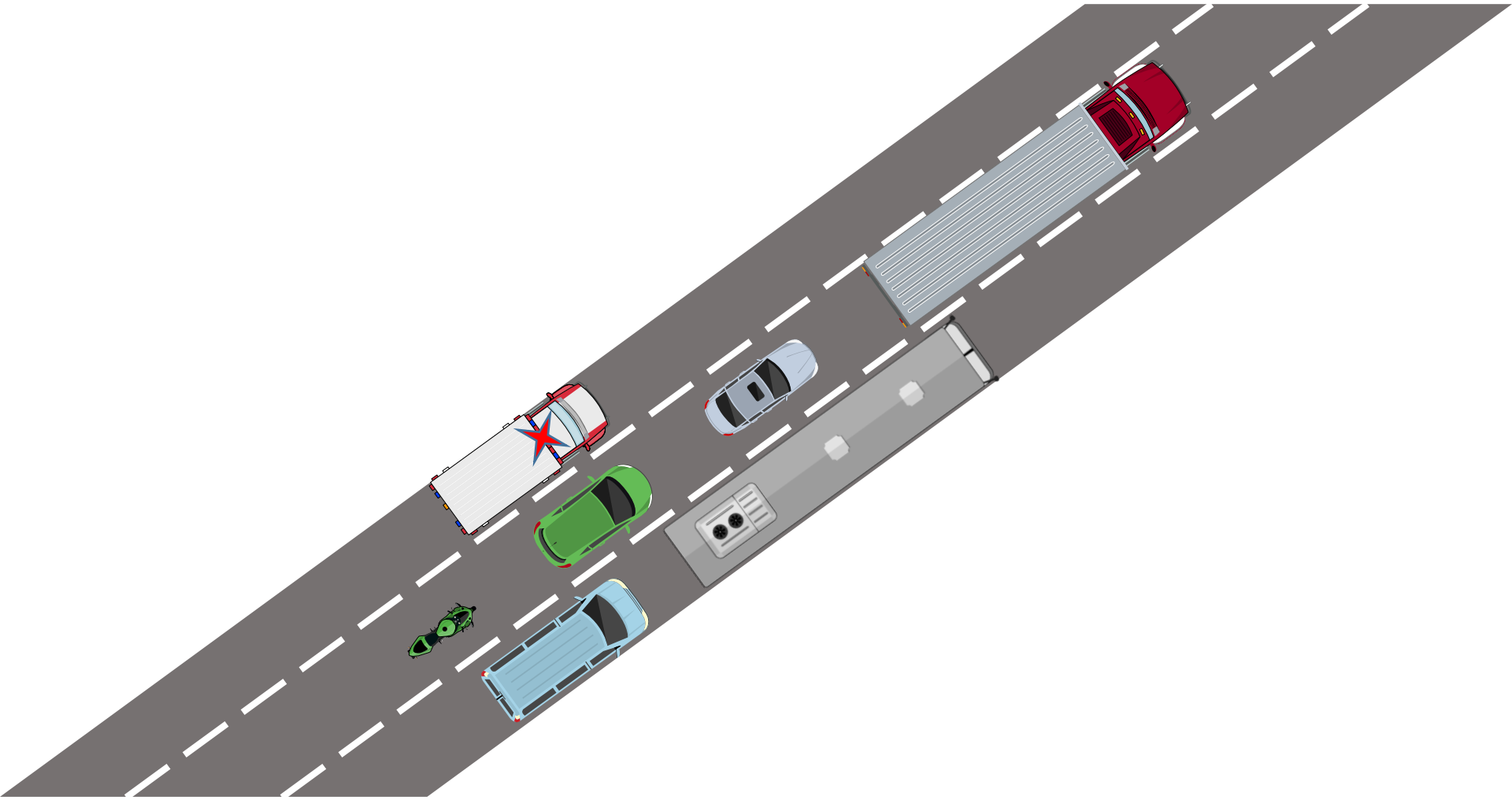
C-roads Spain: ¿Cómo securizar los servicios de transporte inteligente?

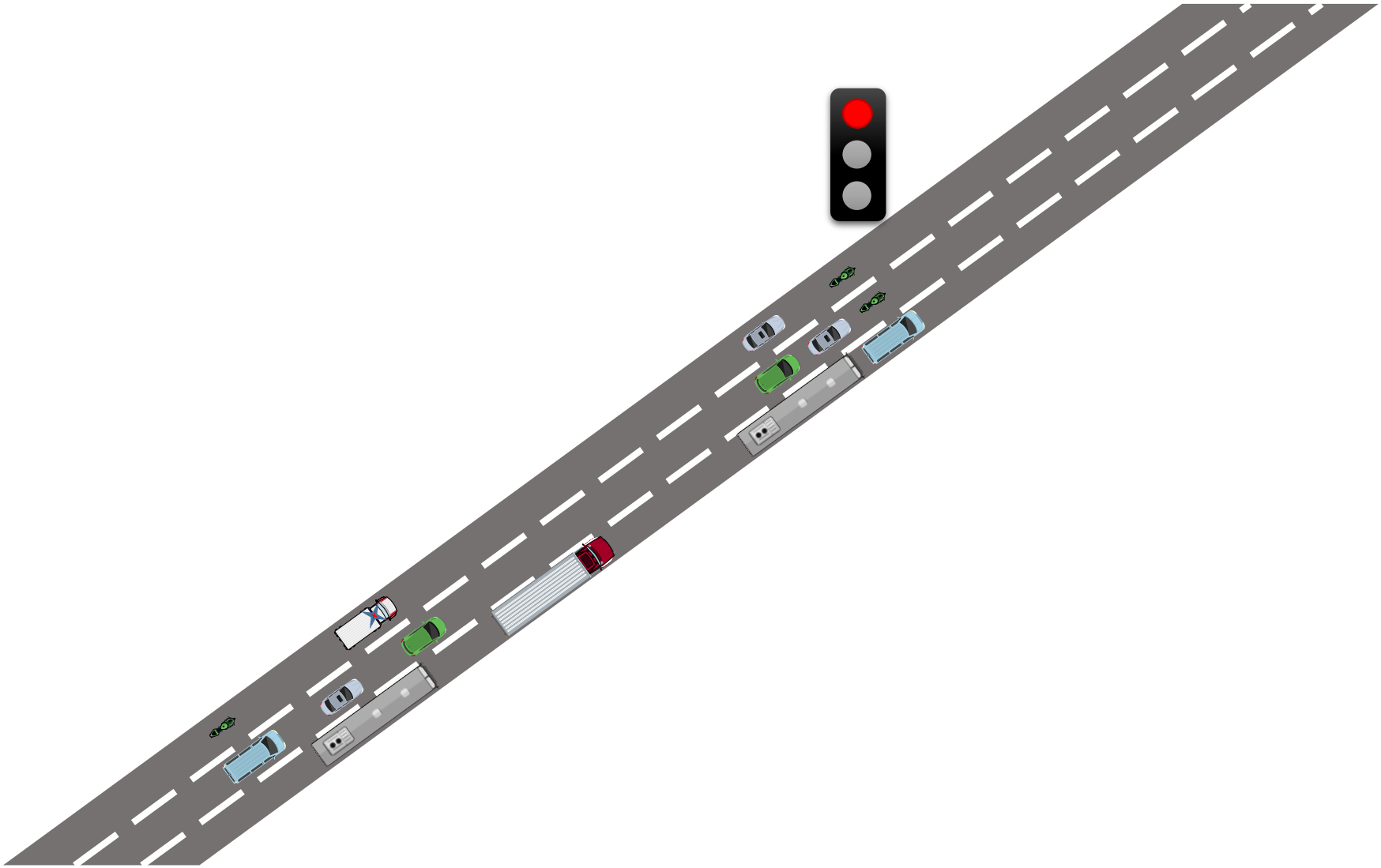
Antonio Rodriguez
inLab.FIB-esCERT UPC | Mayo 2018

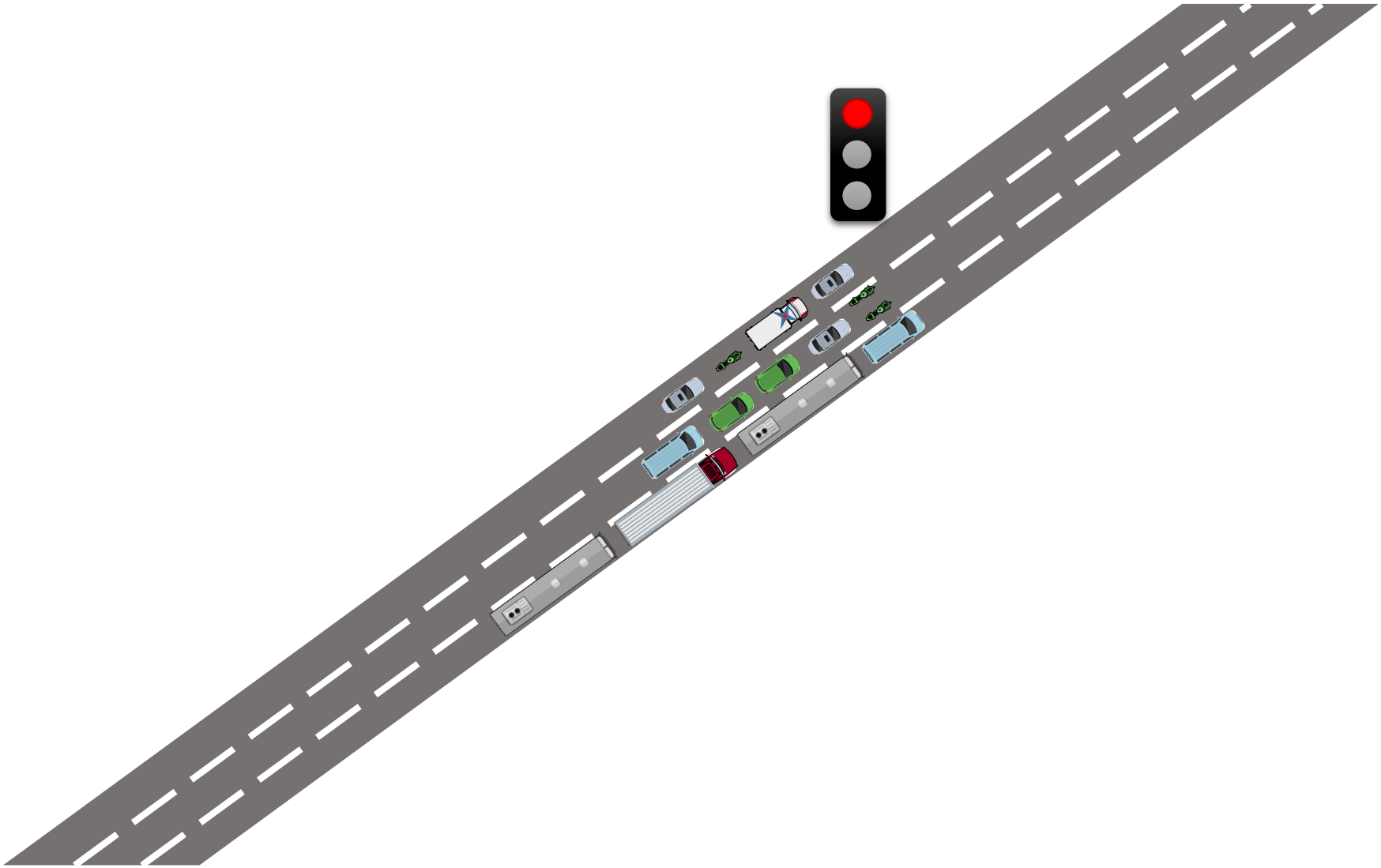


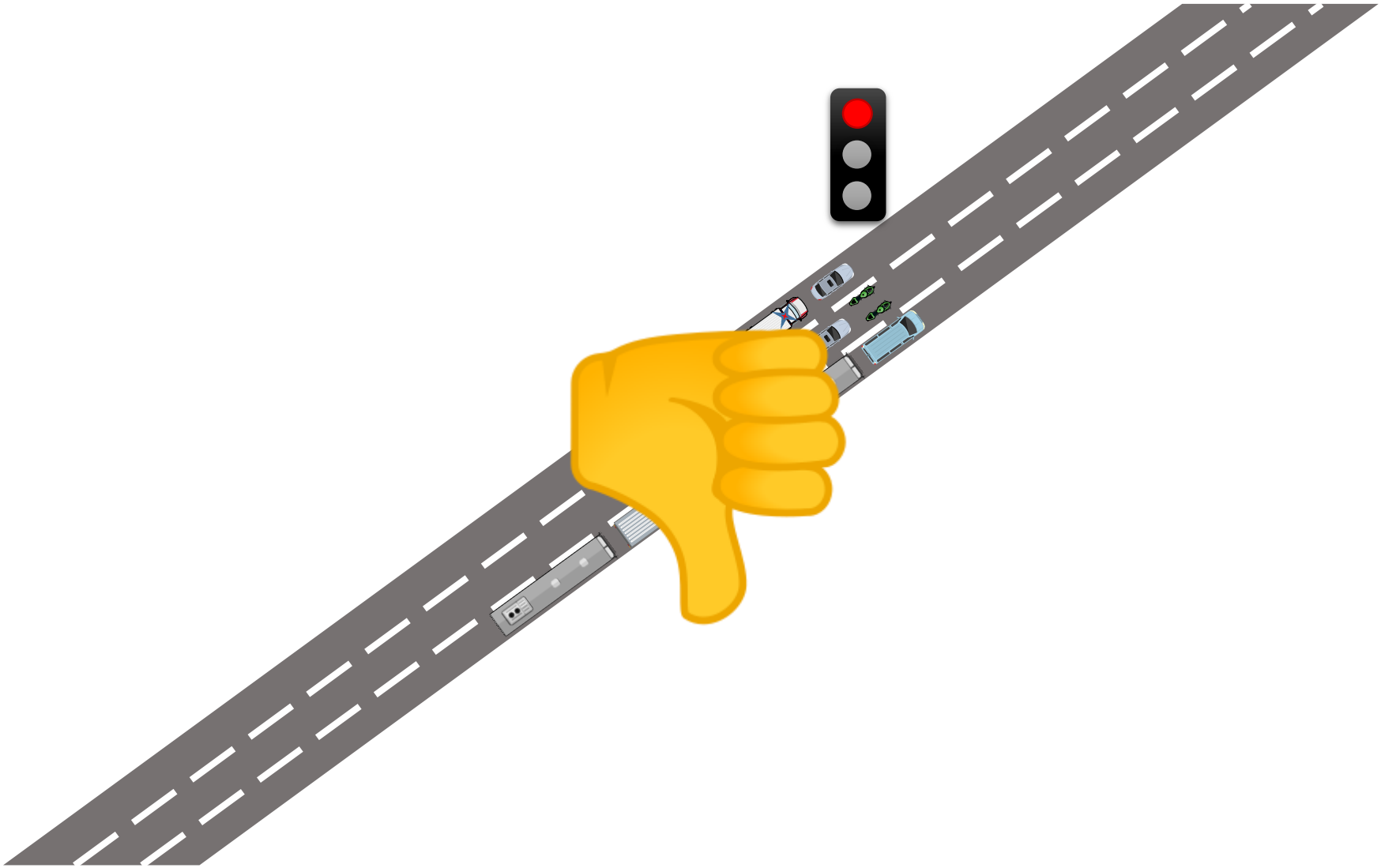






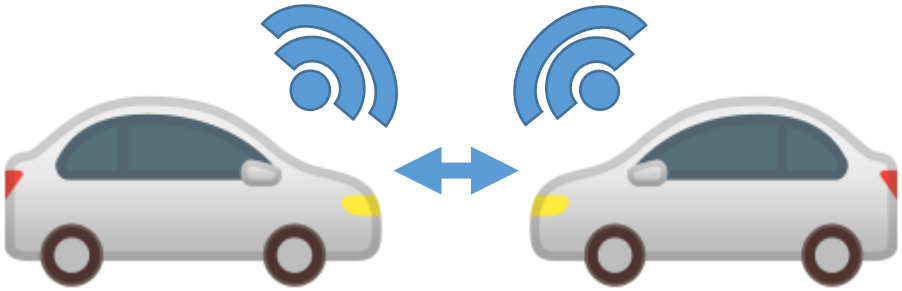






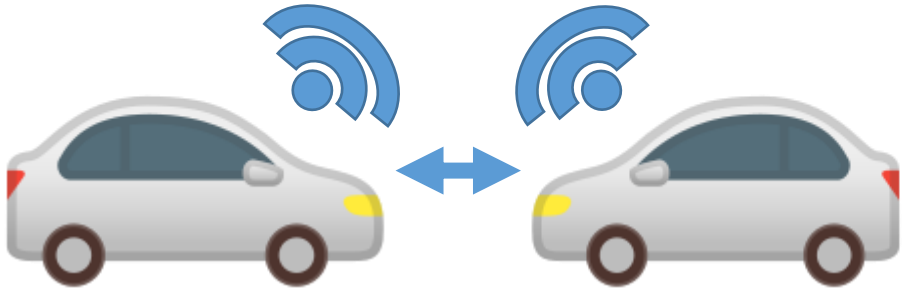
Inteligent Transport Systems (ITS)

Inteligent Transport Systems (ITS)

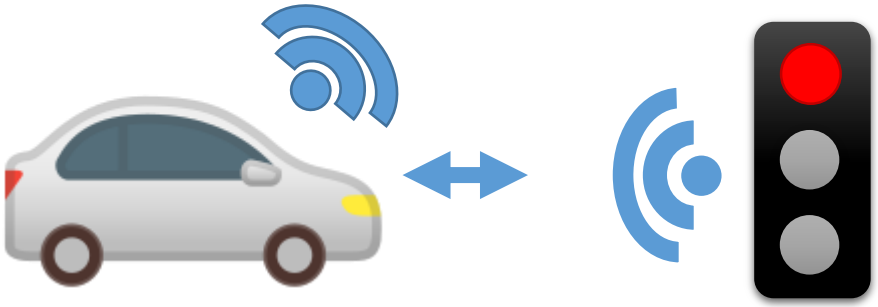


Vehicle to vehicle (V2V)

Inteligent Transport Systems (ITS)

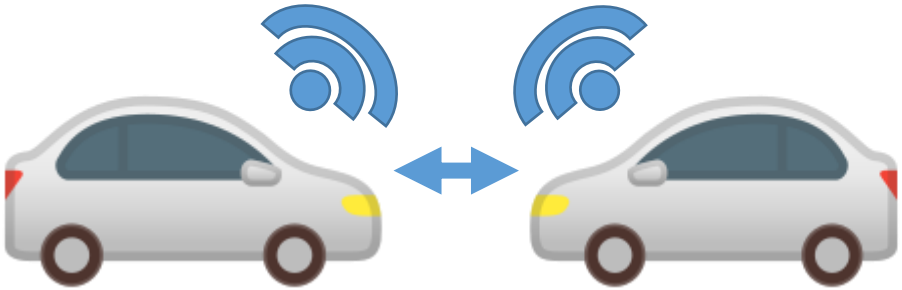


Vehicle to vehicle (V2V)



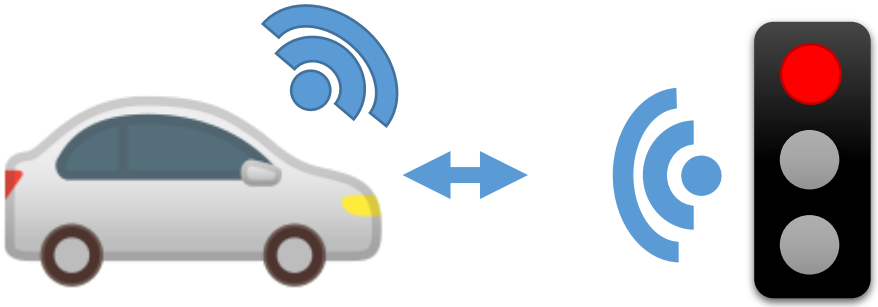
Vehicle to infraestruture (V2I)

Inteligent Transport Systems (ITS)

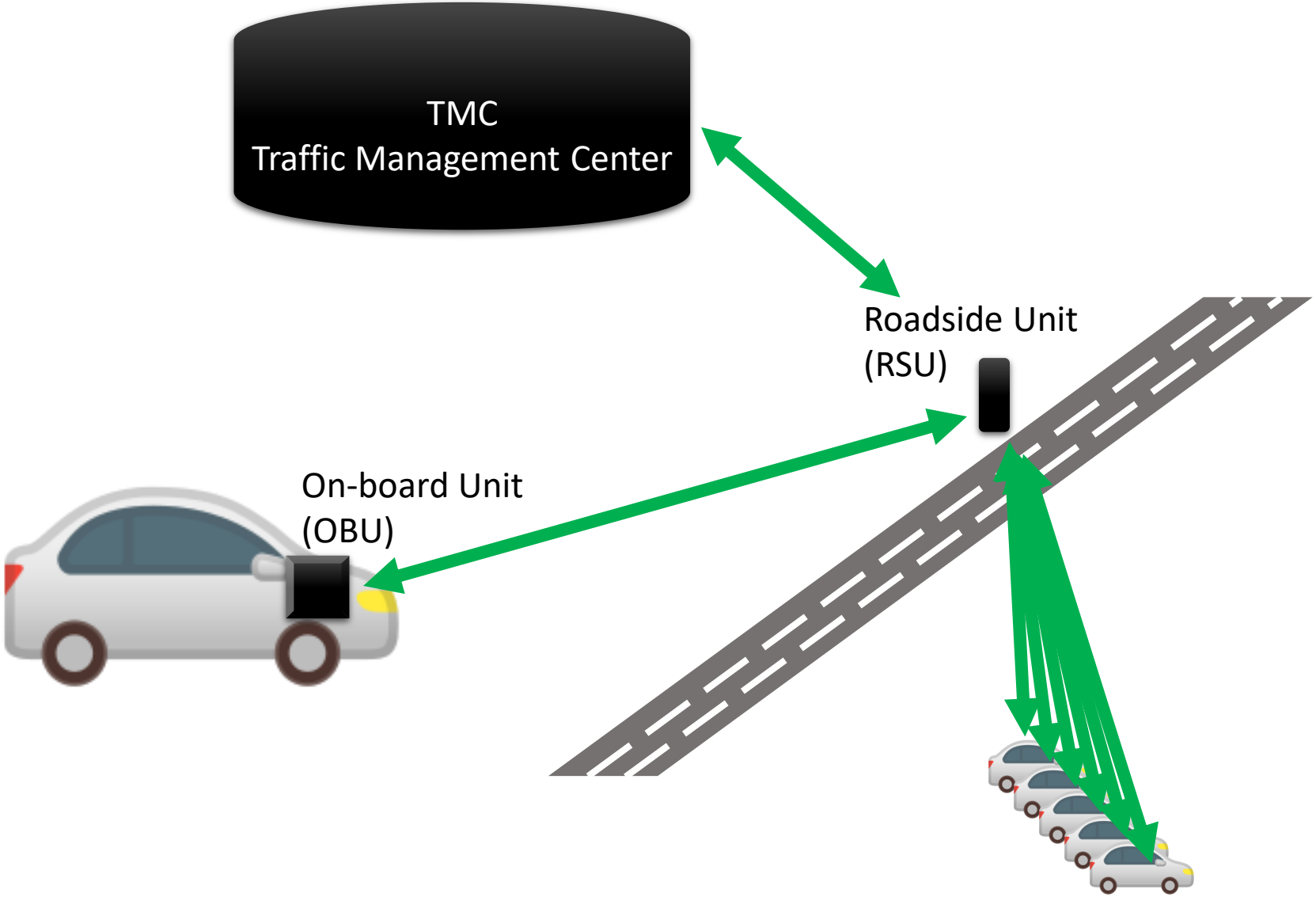


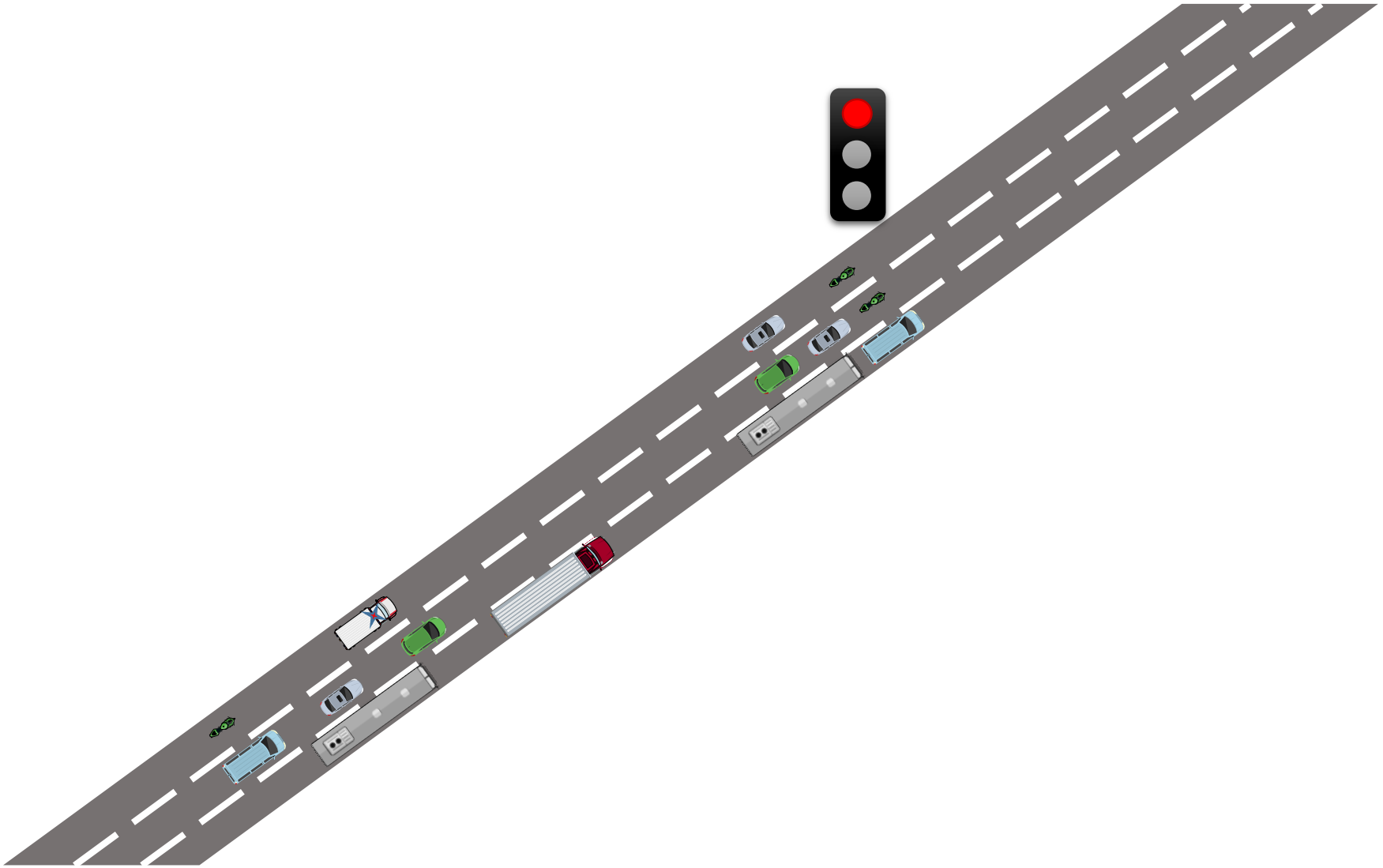
Vehicle to vehicle (V2V)

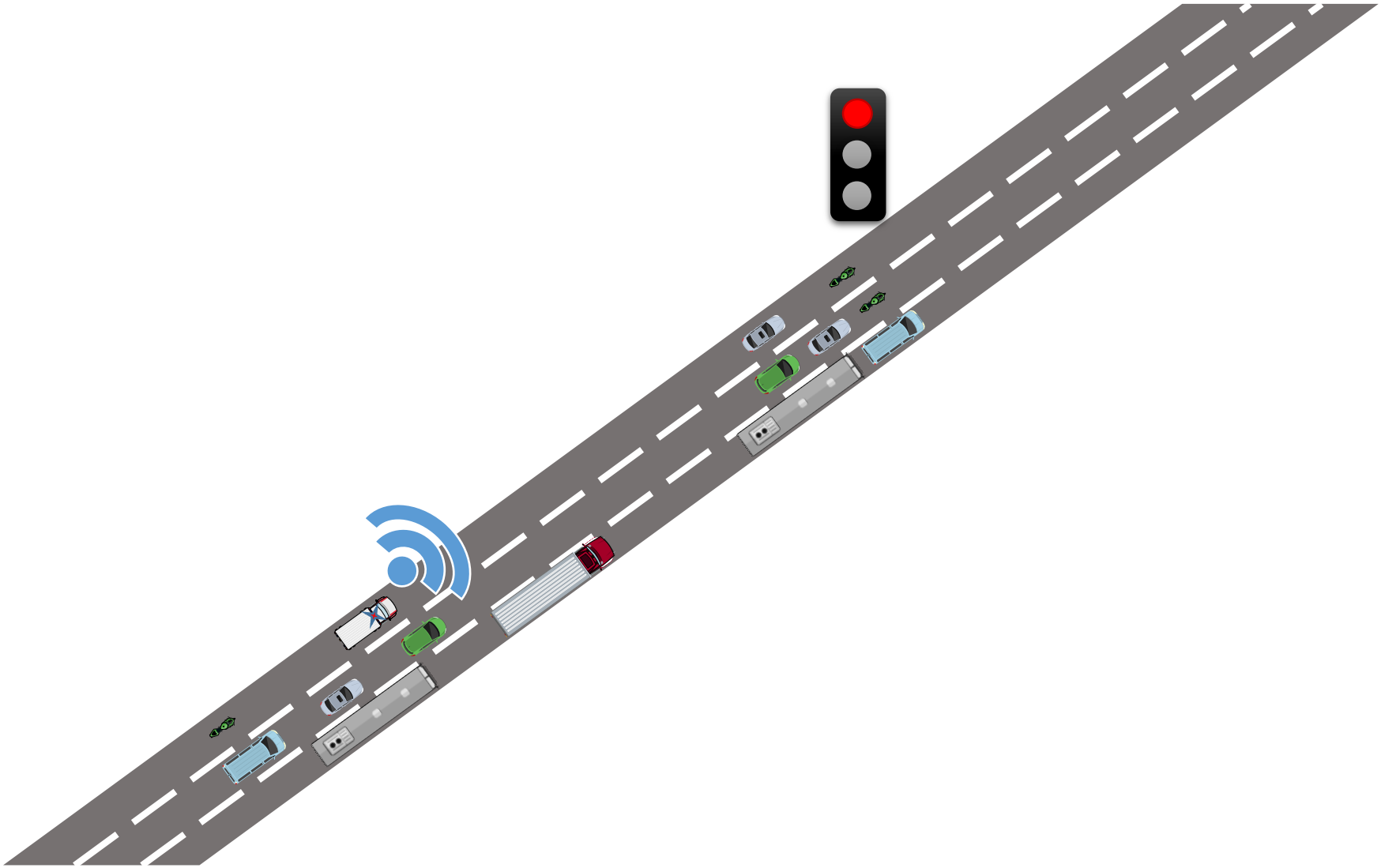
Vehicle to anything! (V2X)

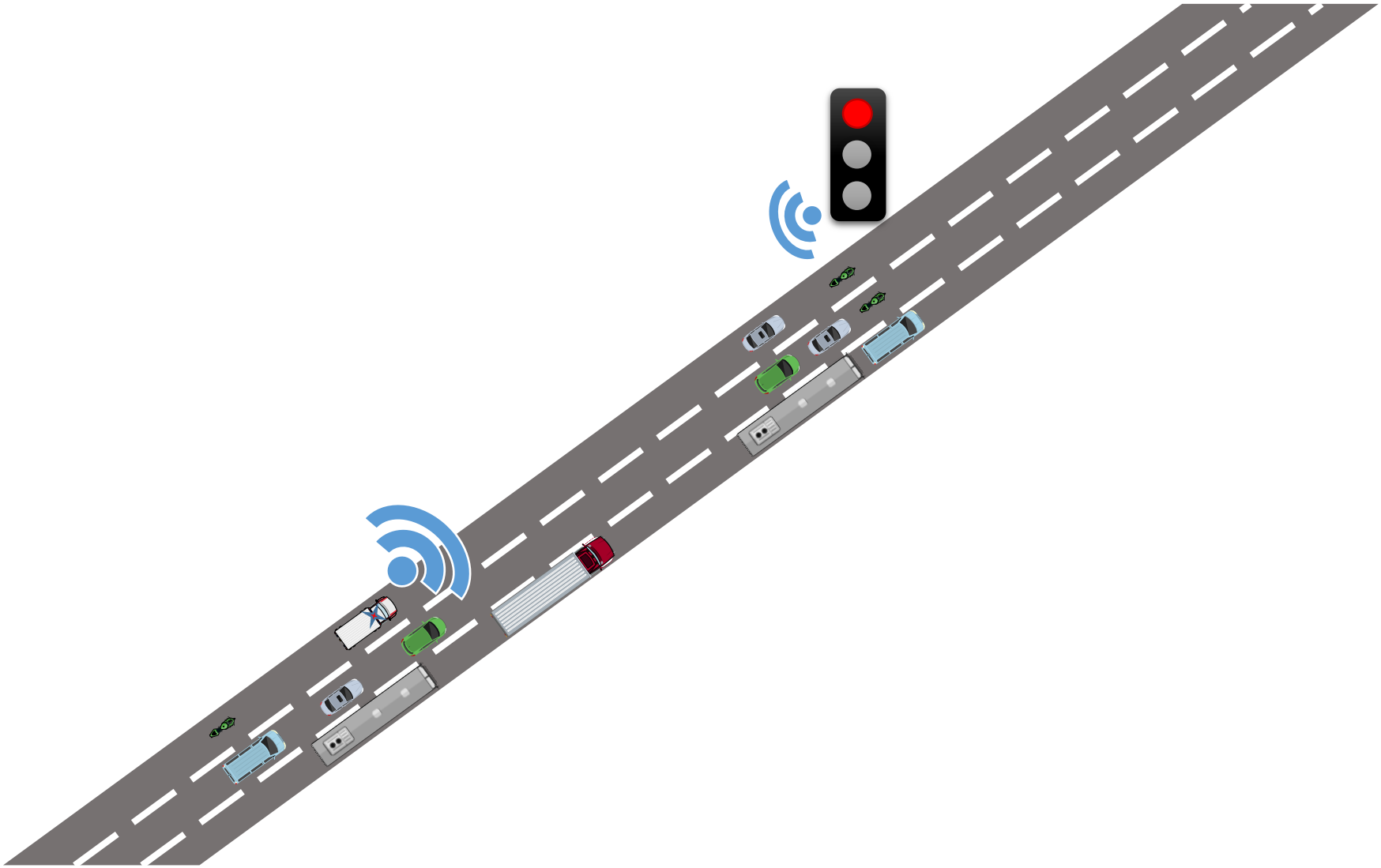


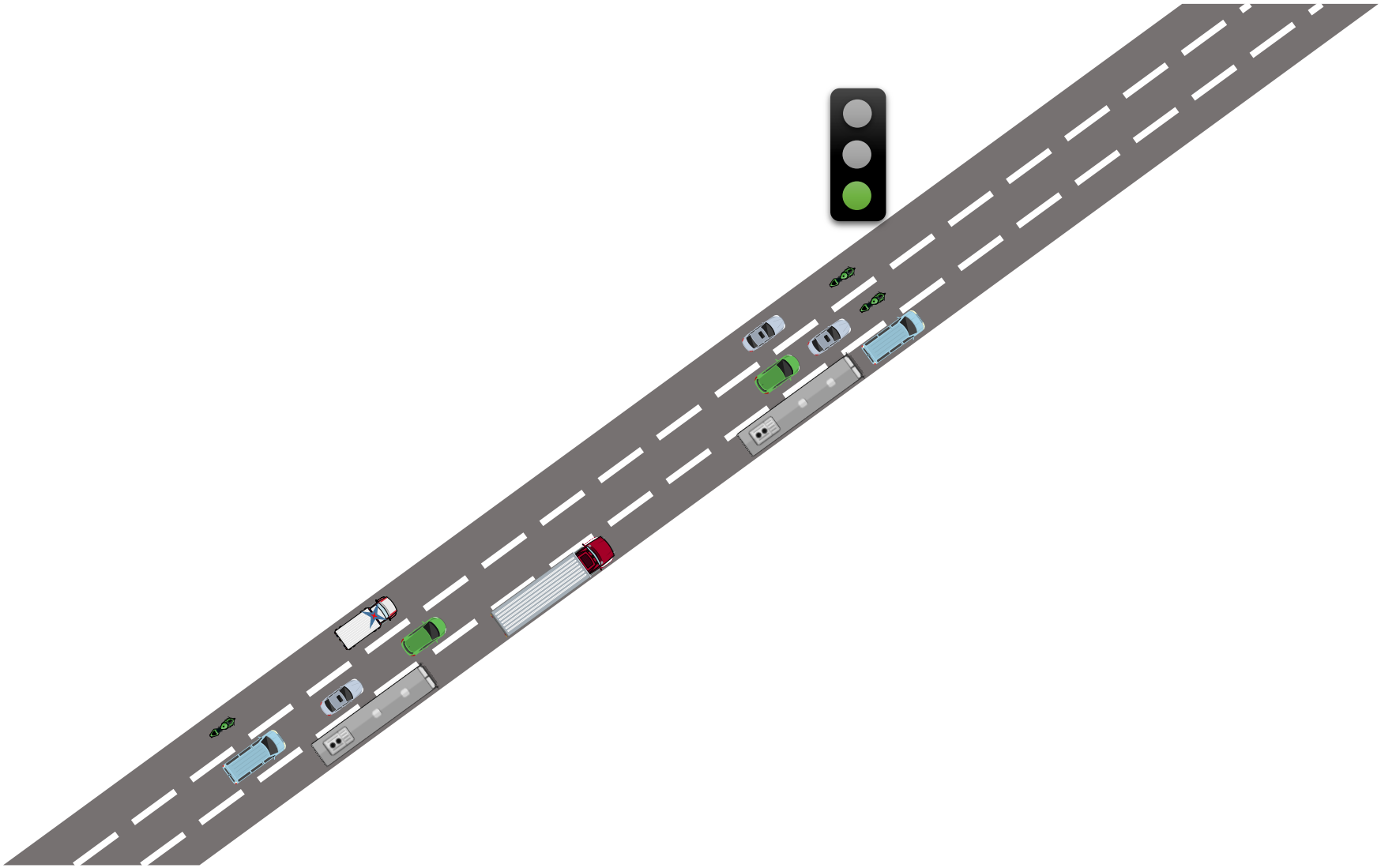
Vehicle to infraestruture (V2I)

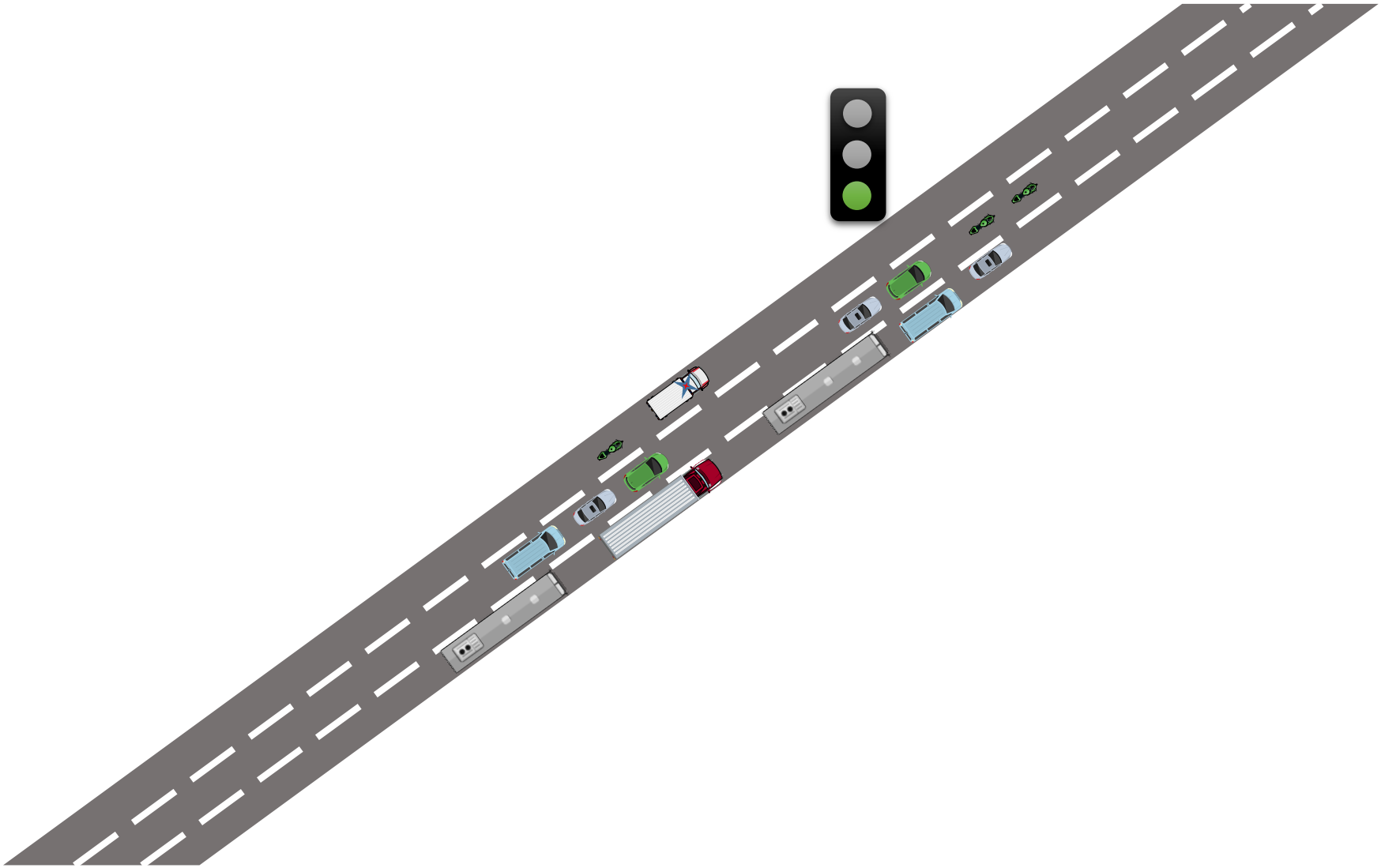

TMC
Traffic Management Center
Roadside Unit
(RSU)
On-board Unit
(OBU)

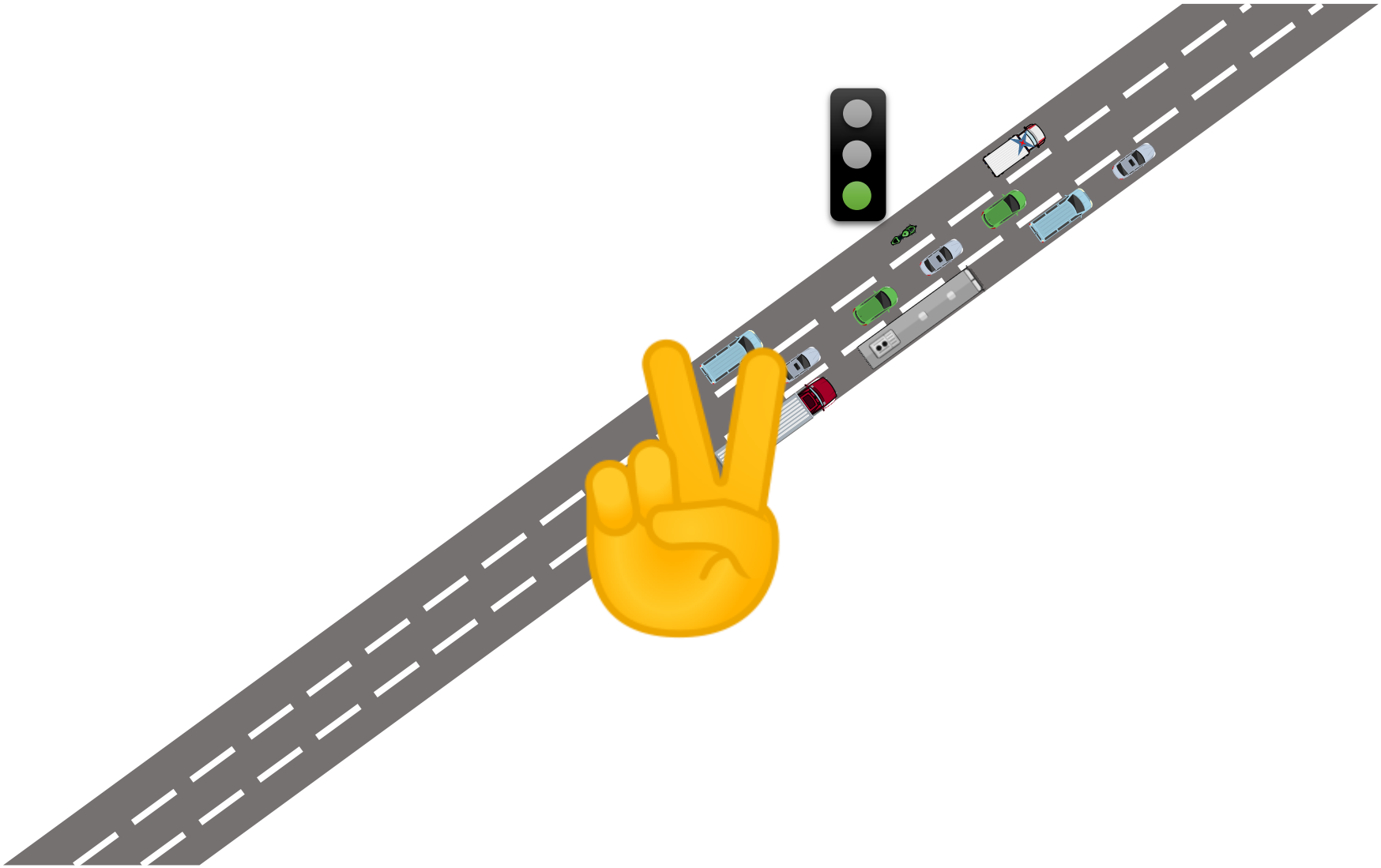


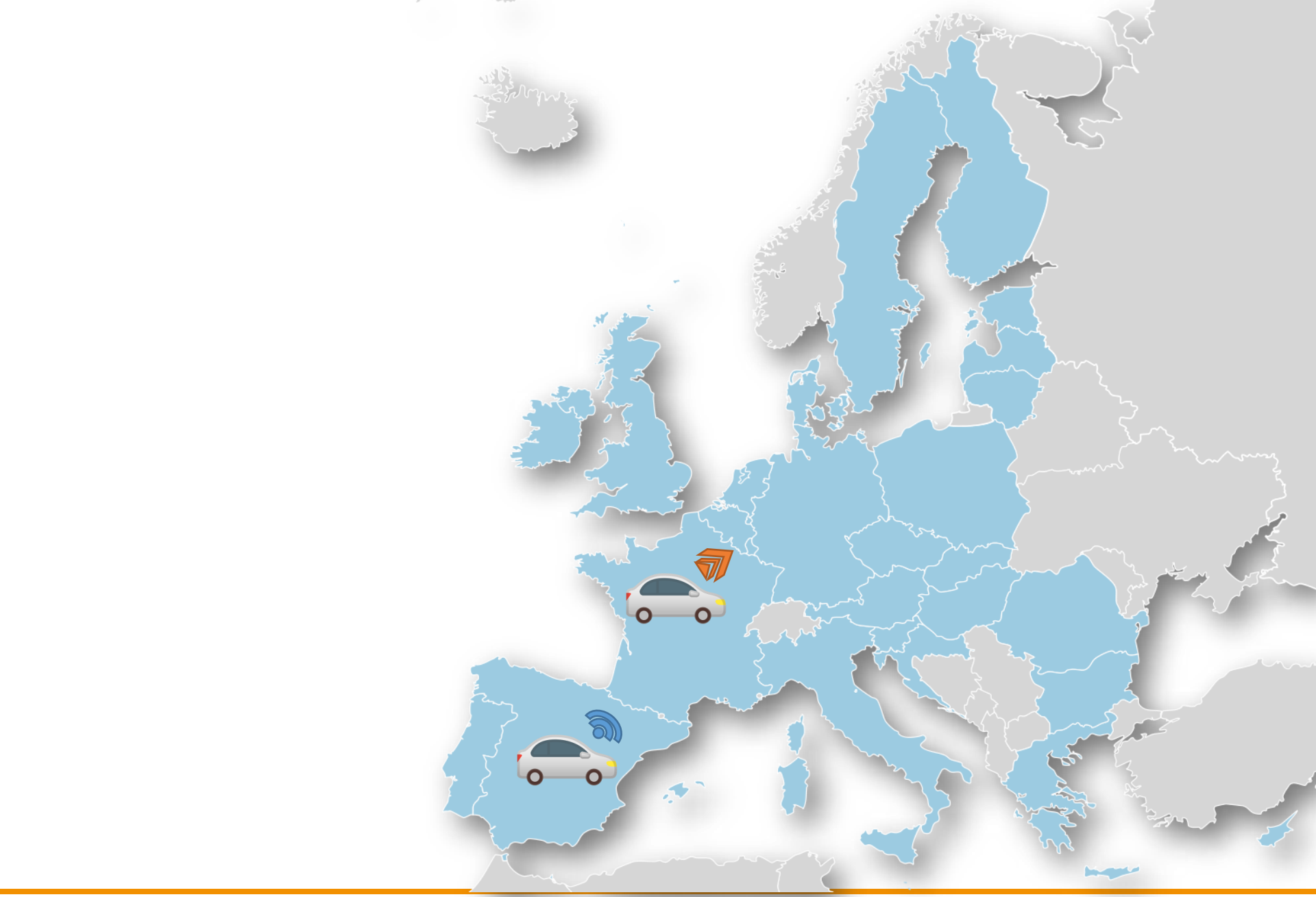










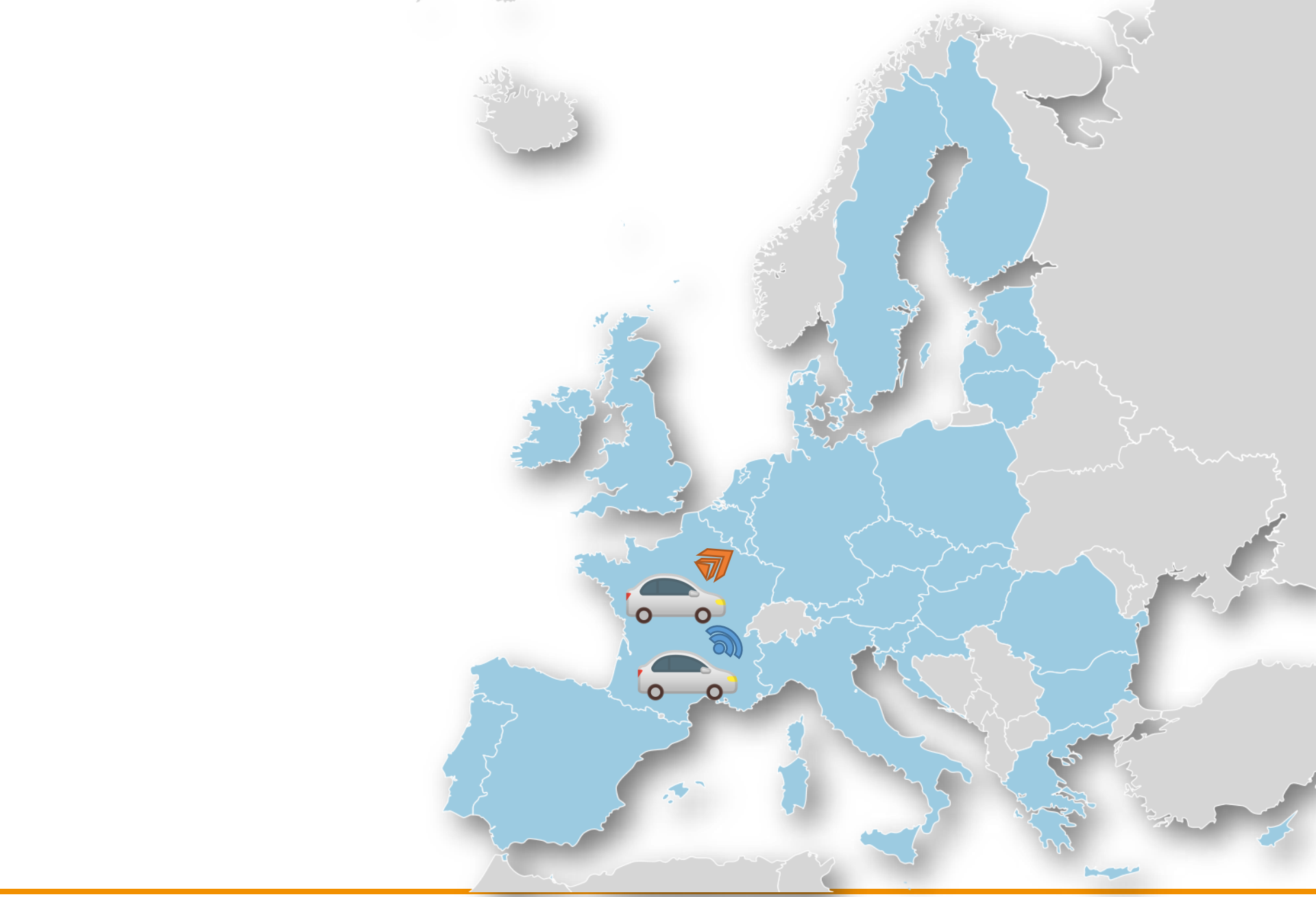


RedIRIS

inLab FIB talent & tech

ESCERT

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

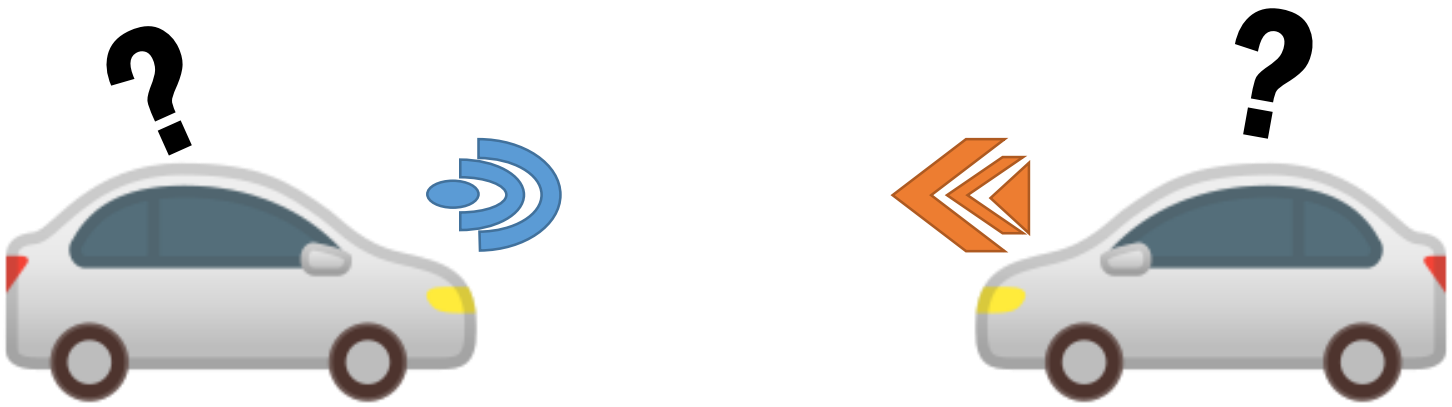


RedIRIS

inLab FIB talent & tech

ESCERT

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH



C-ROADS

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

C-ROADS

Varios pilotos agrupados por países

C-ROADS SPAIN

C-ROADS SPAIN

Participantes

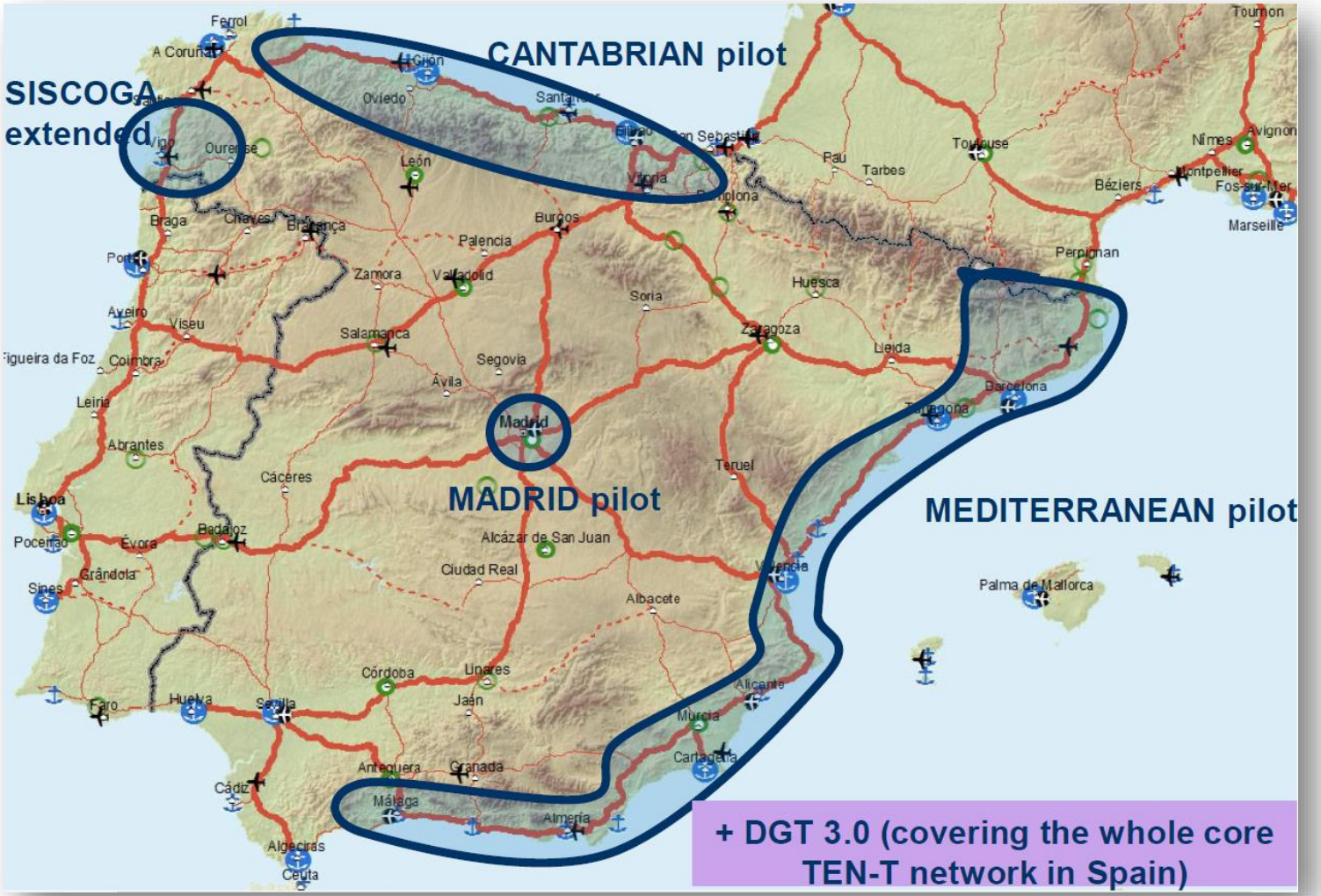
Autoridades públicas

Sector privado

Universidades

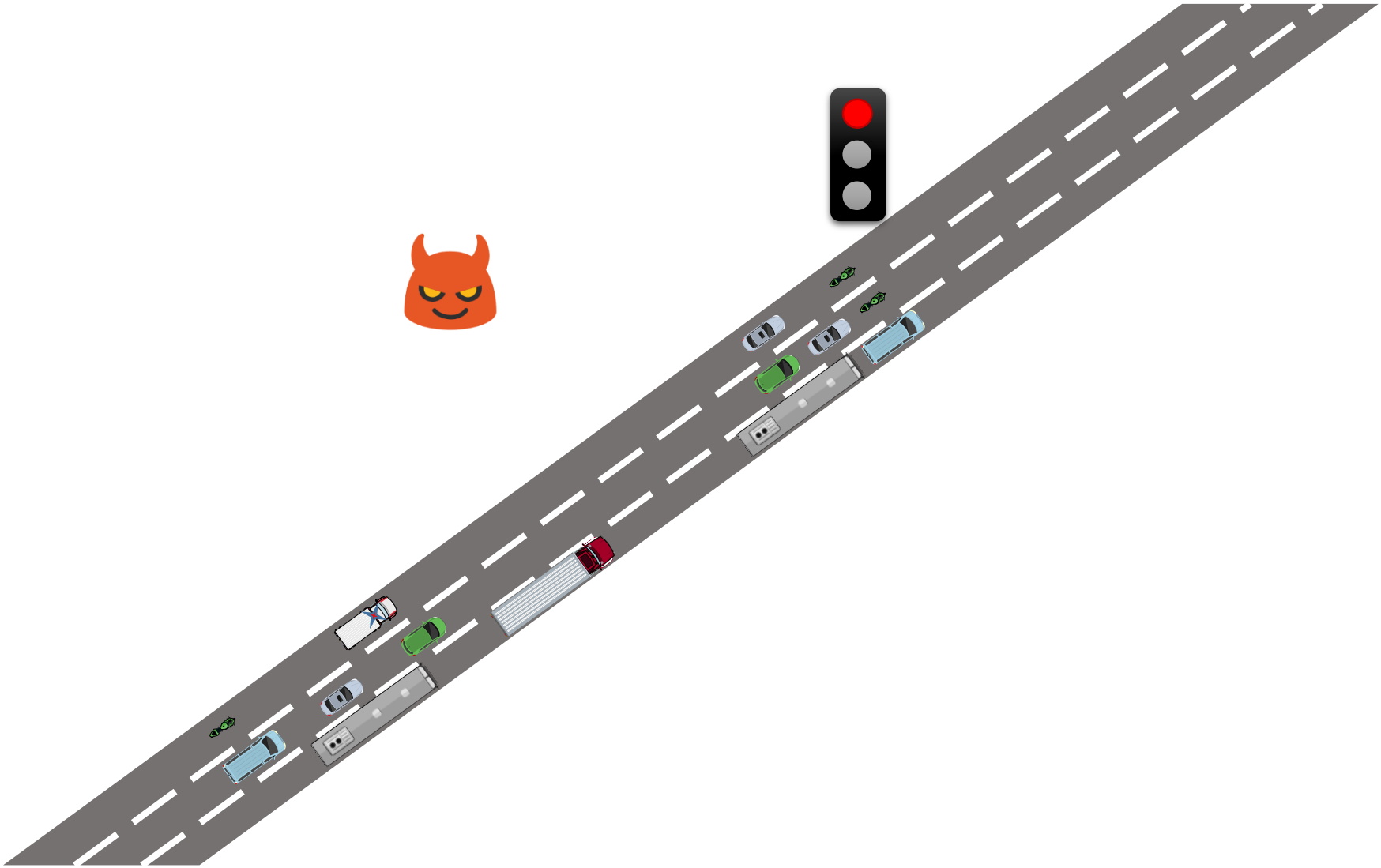
C-ROADS SPAIN

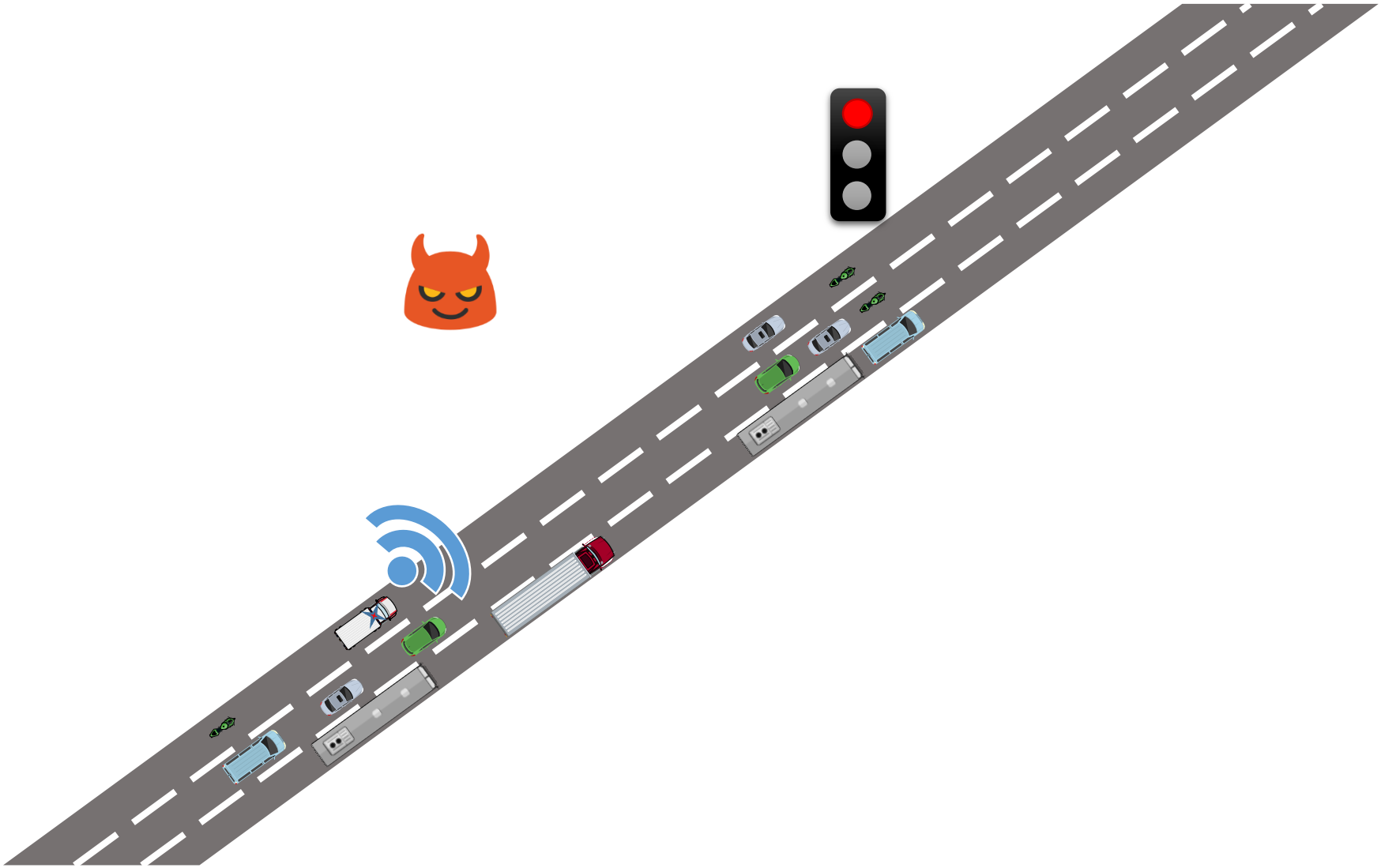
Pilotos

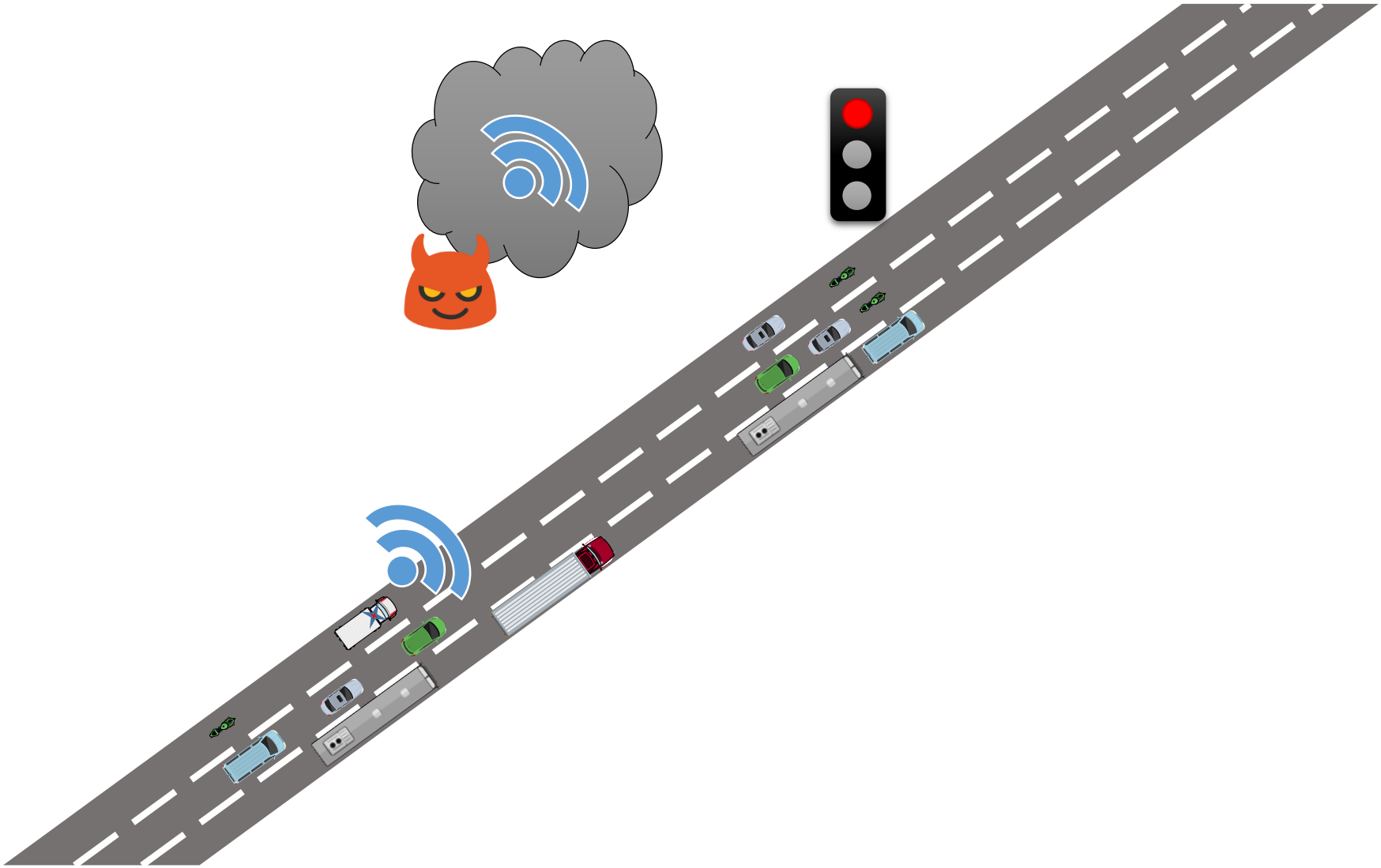


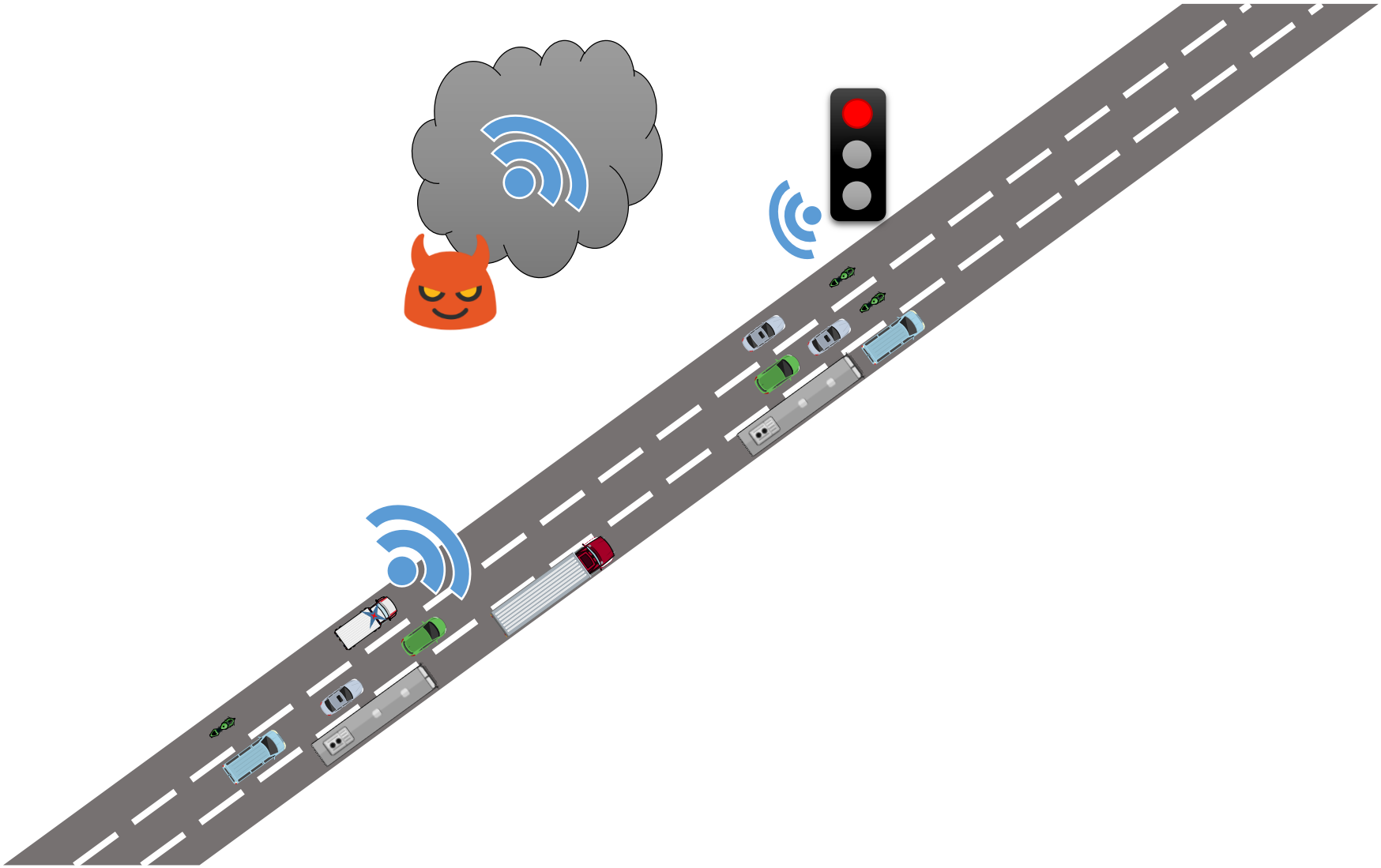
Seguridad?

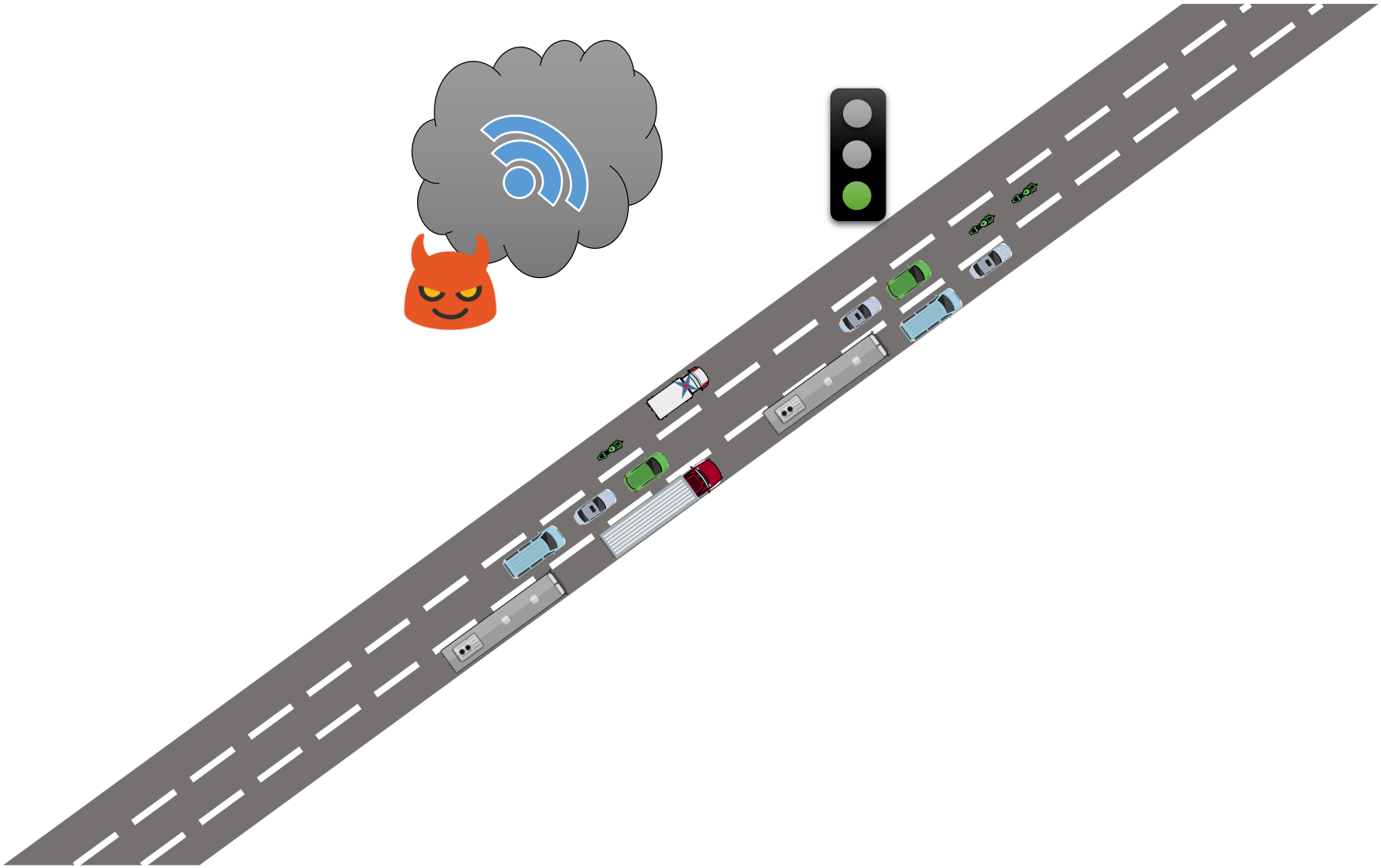
Autenticidad?

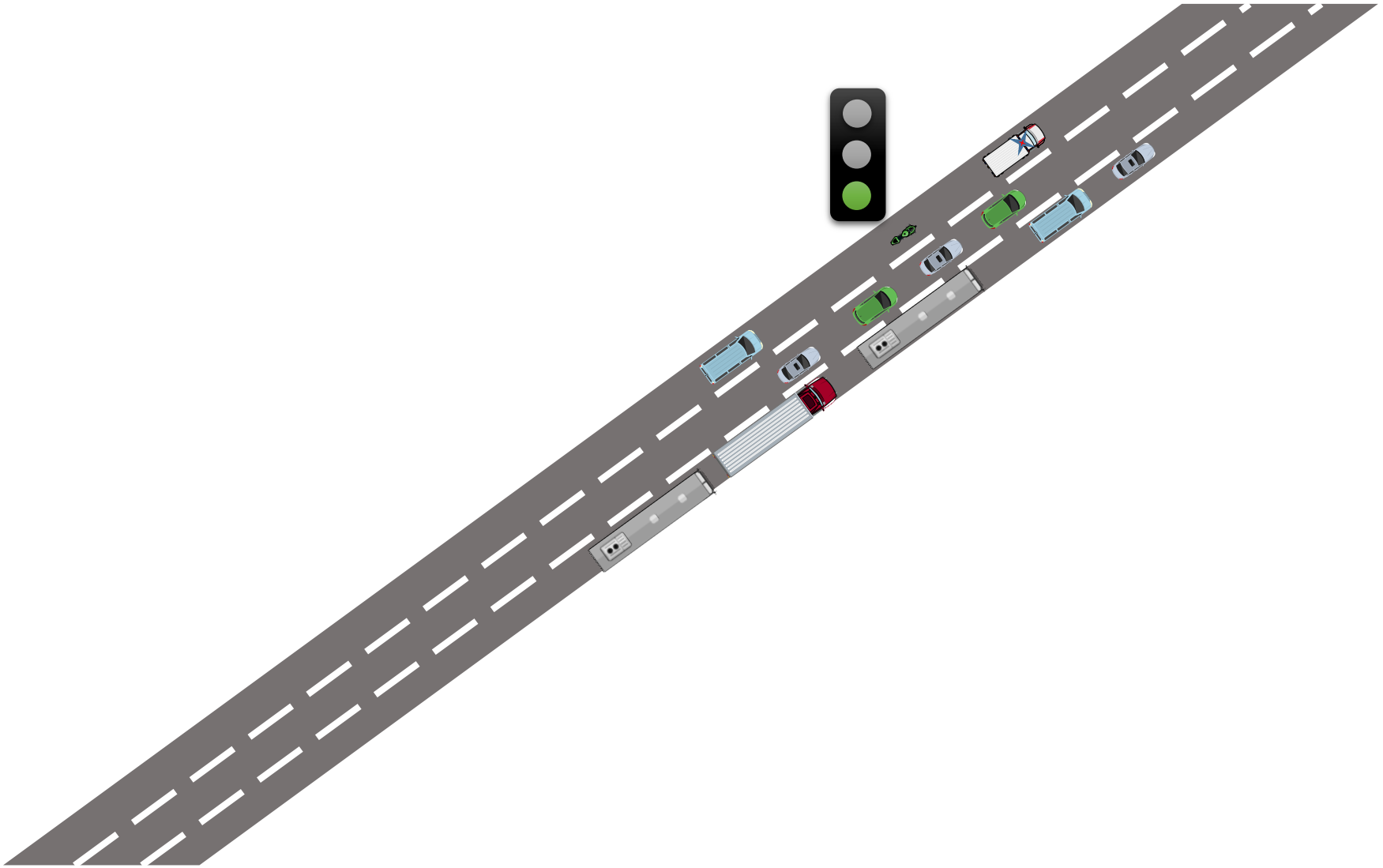


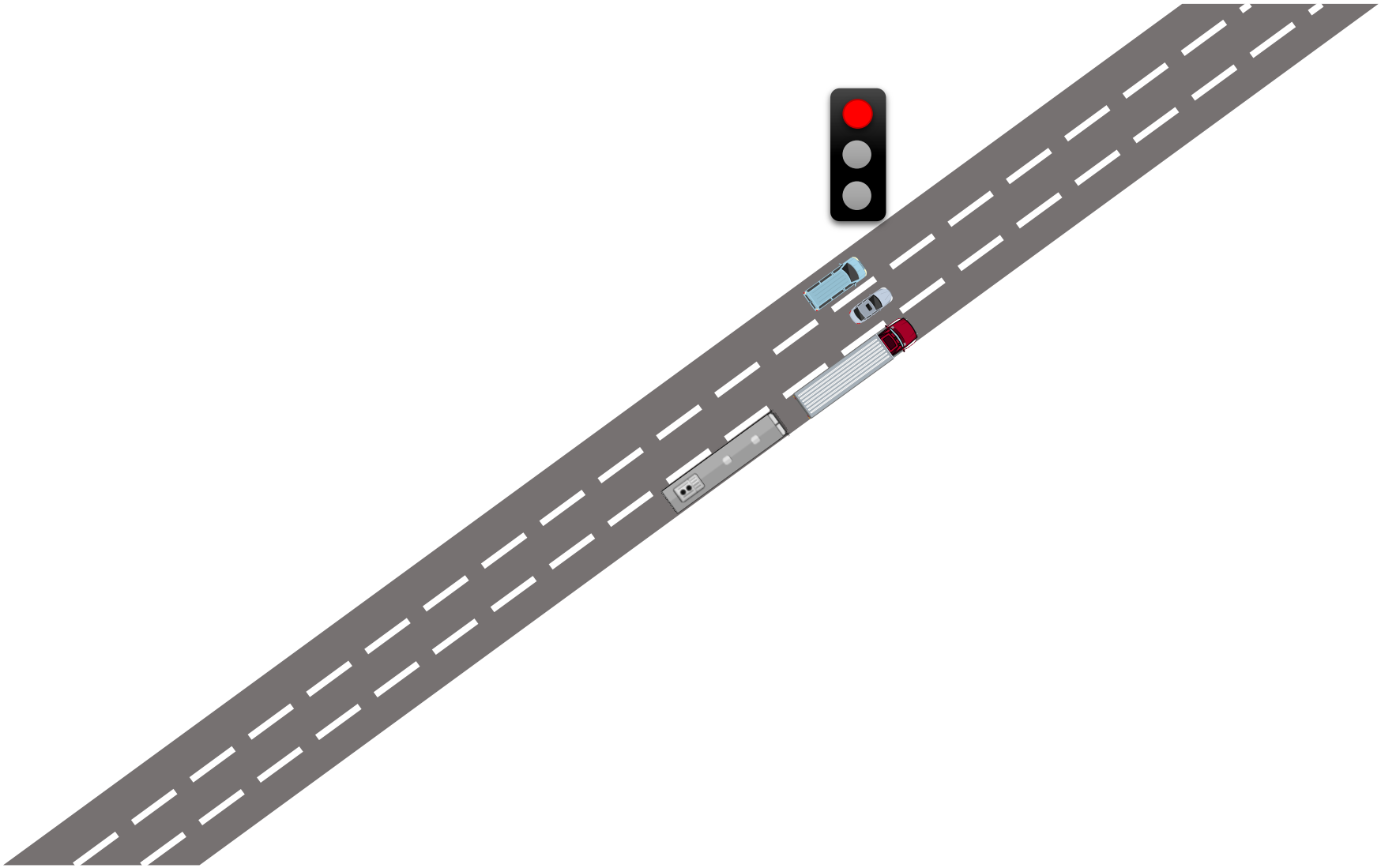


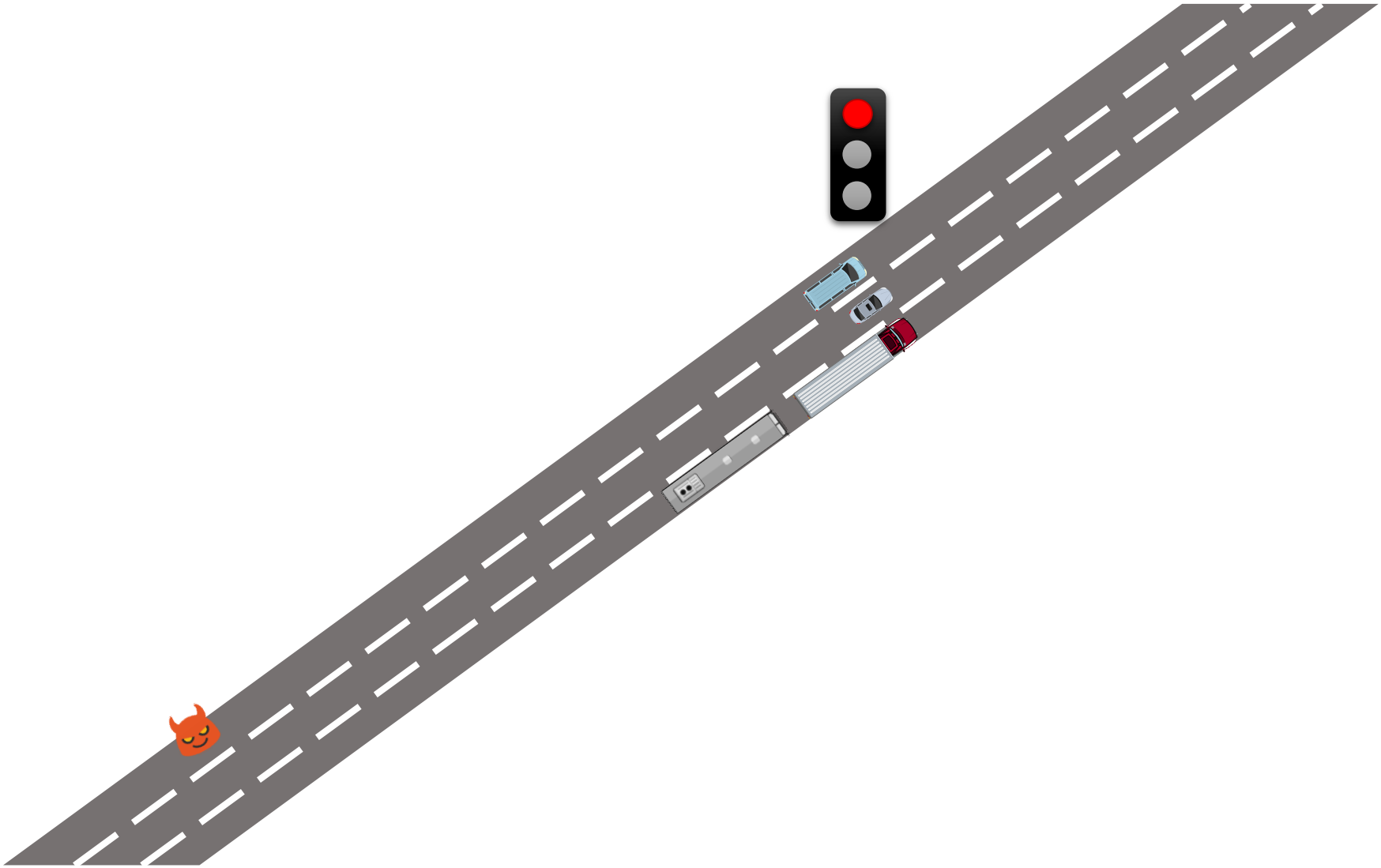


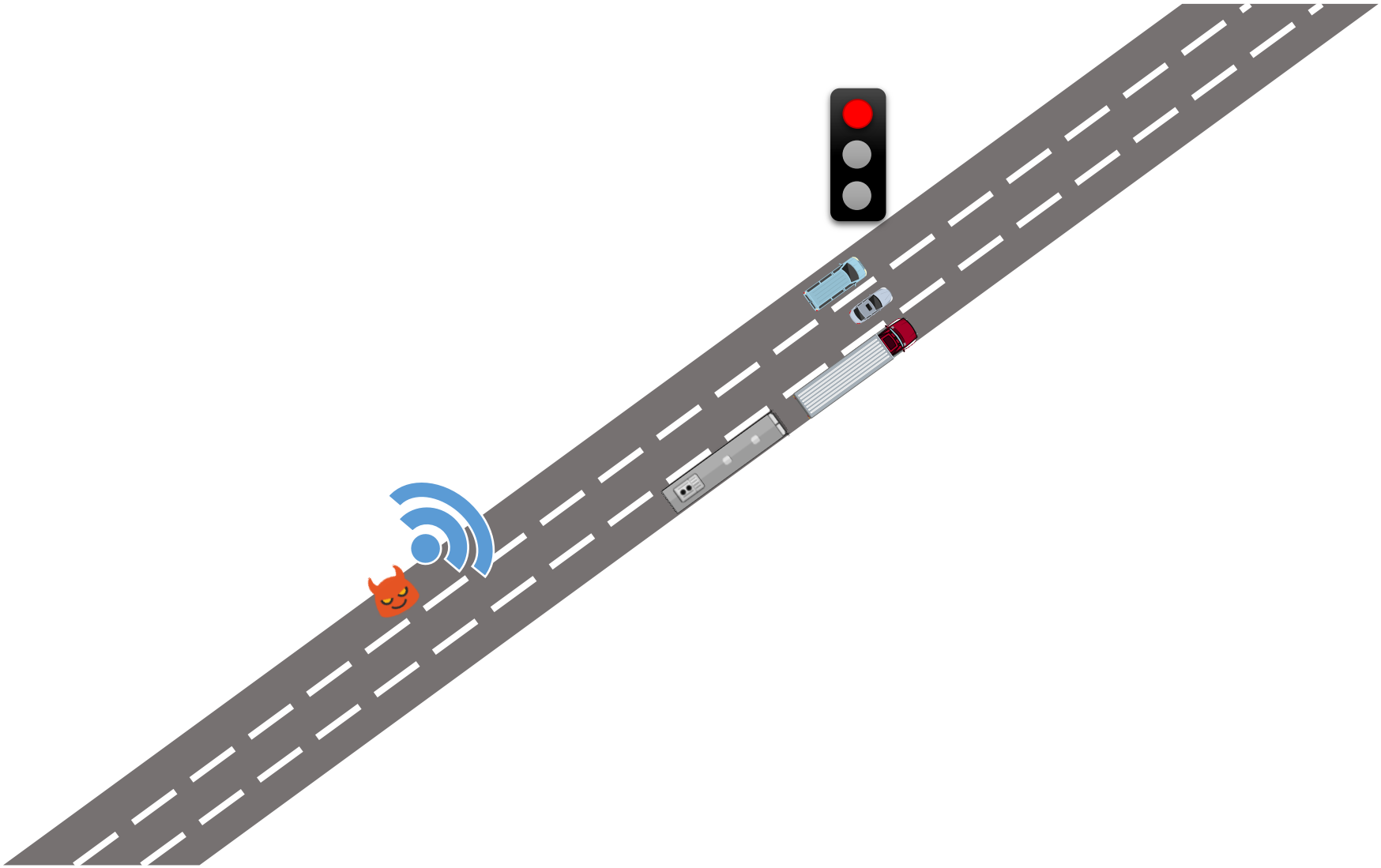


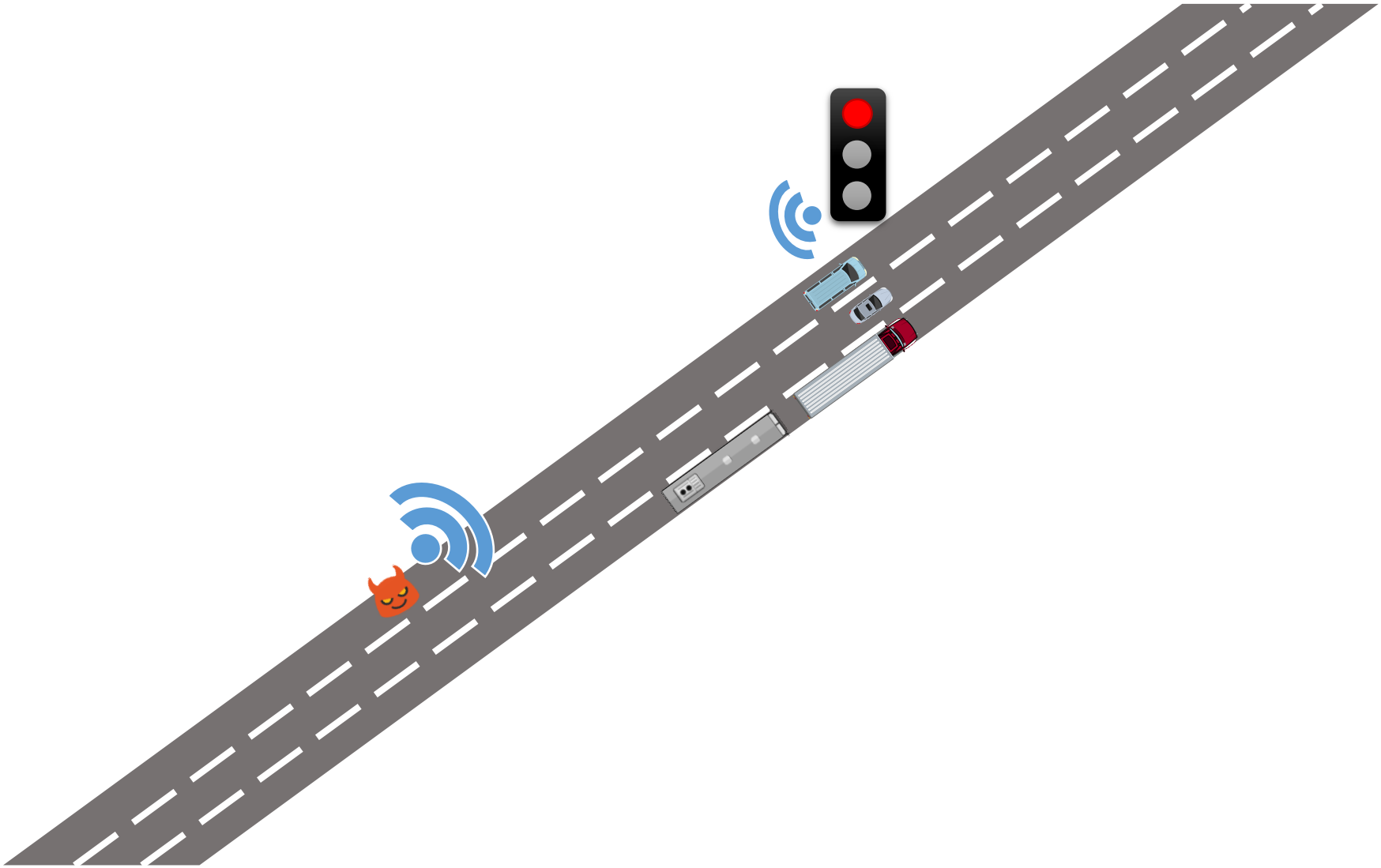


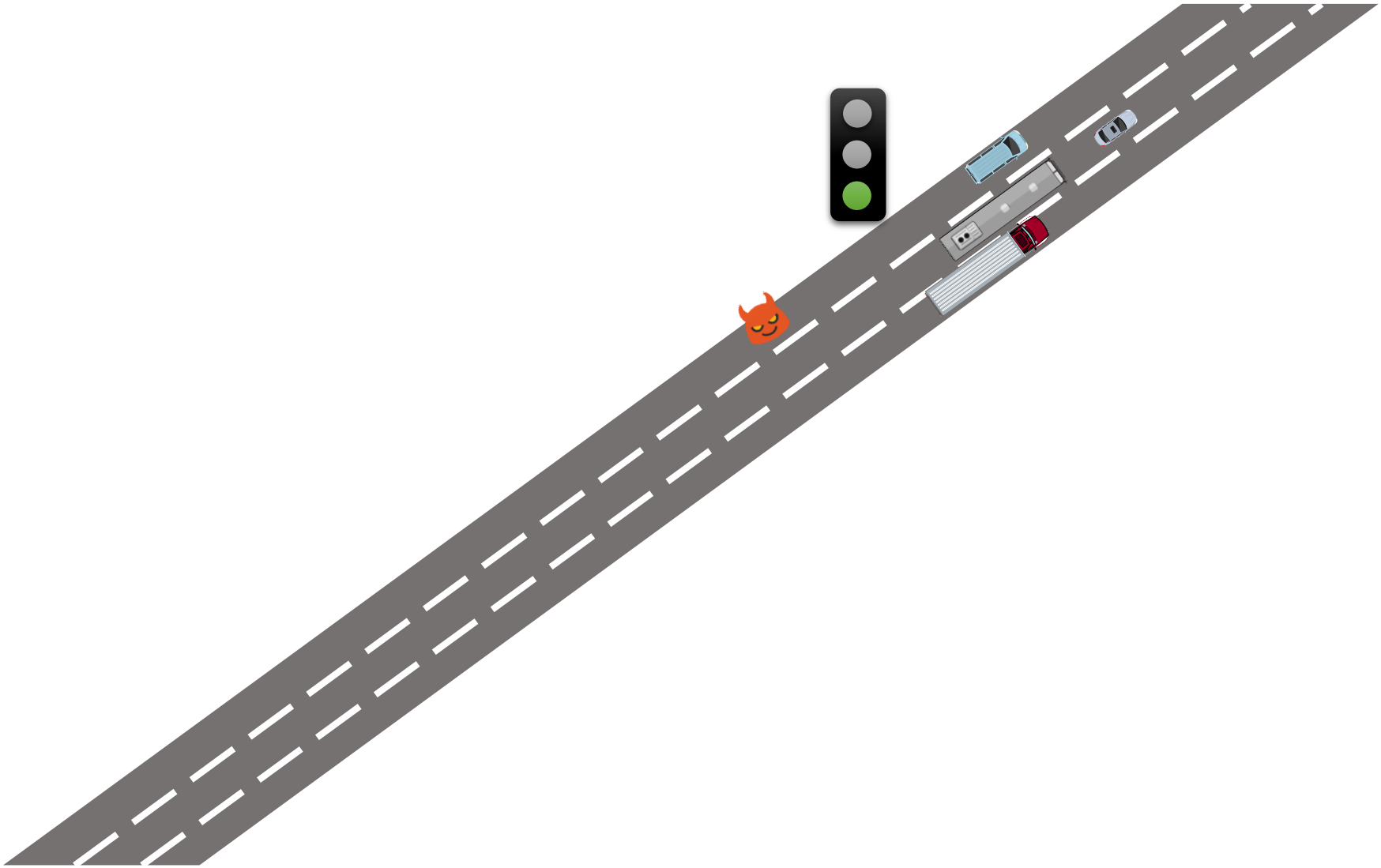


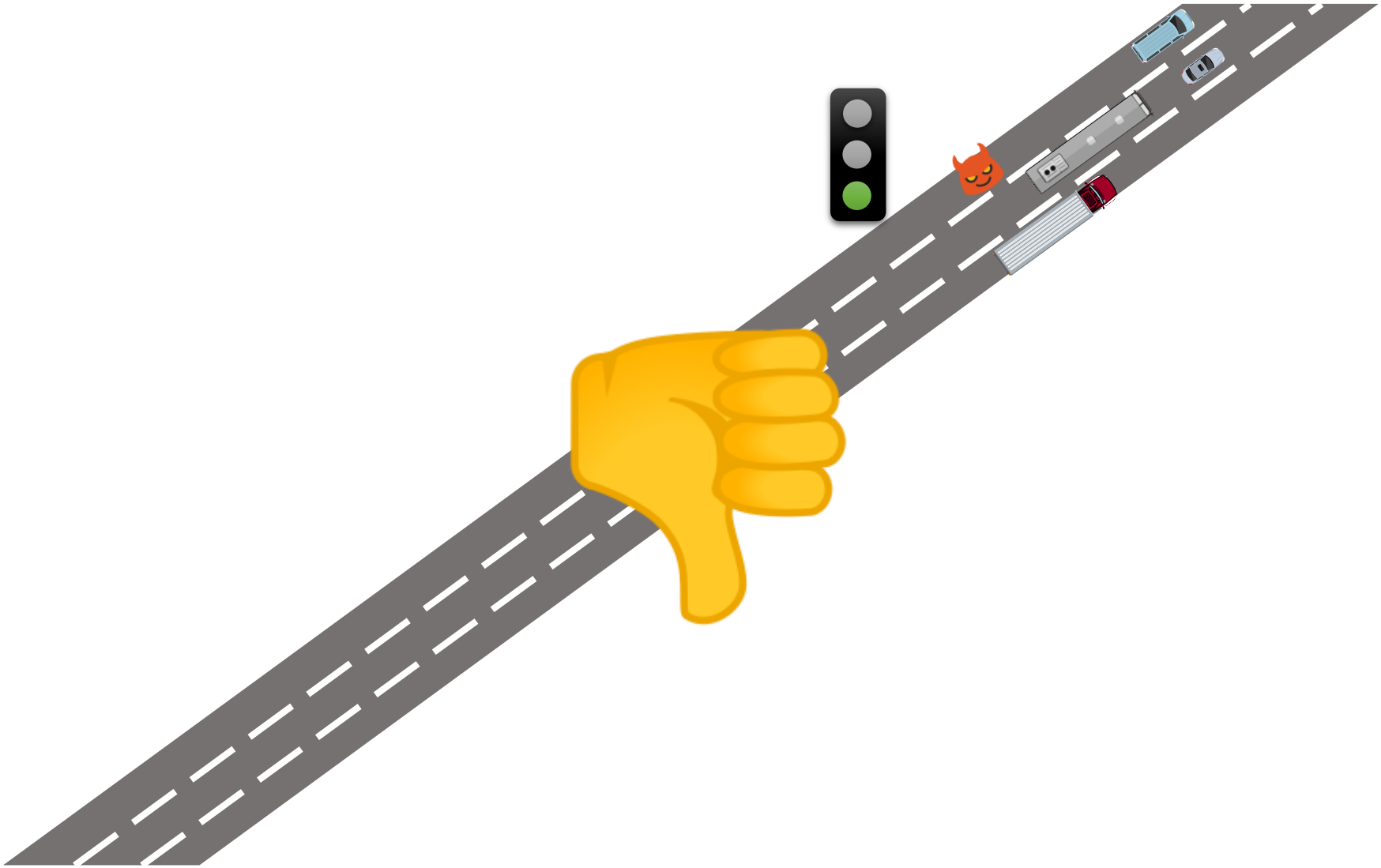




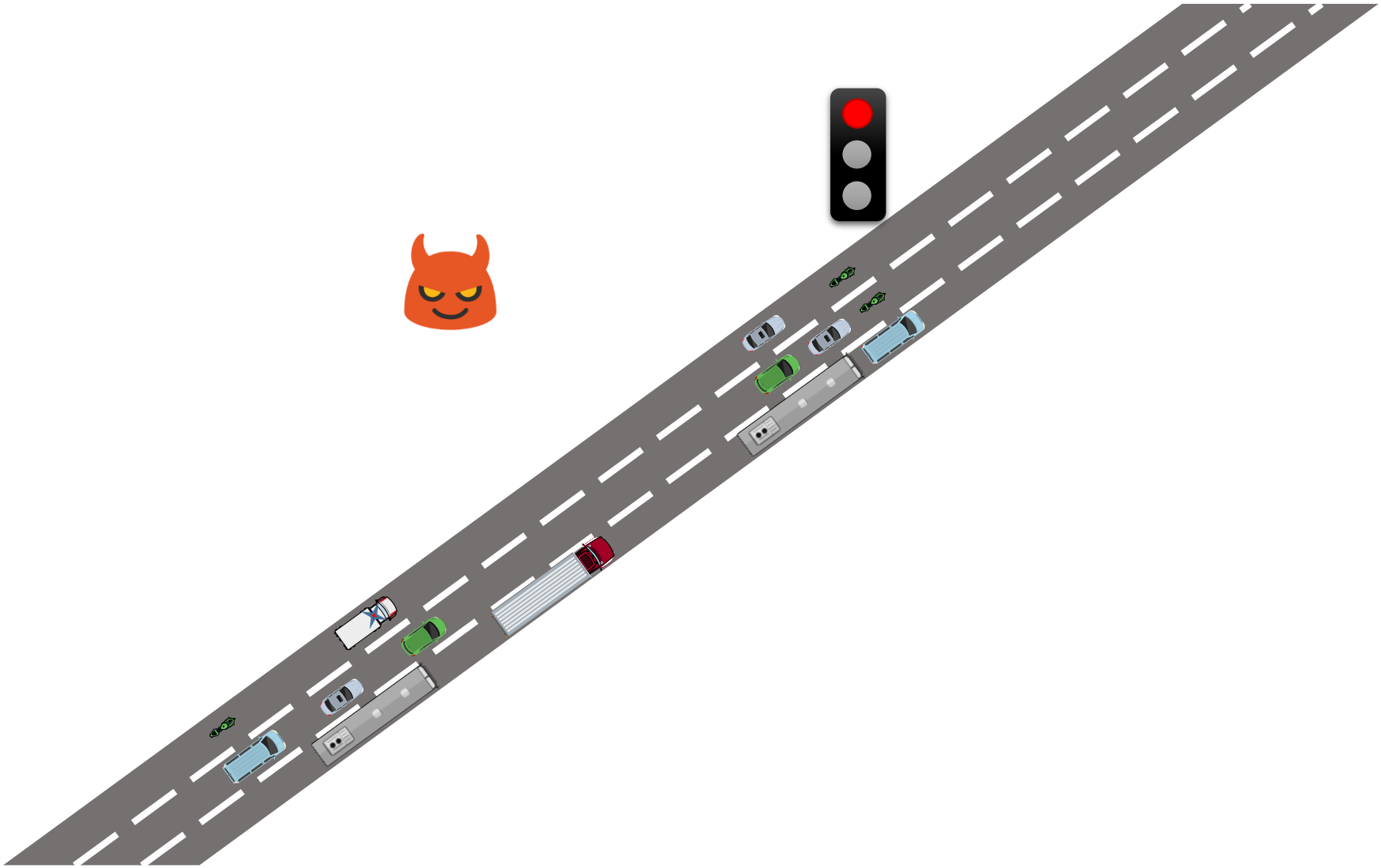


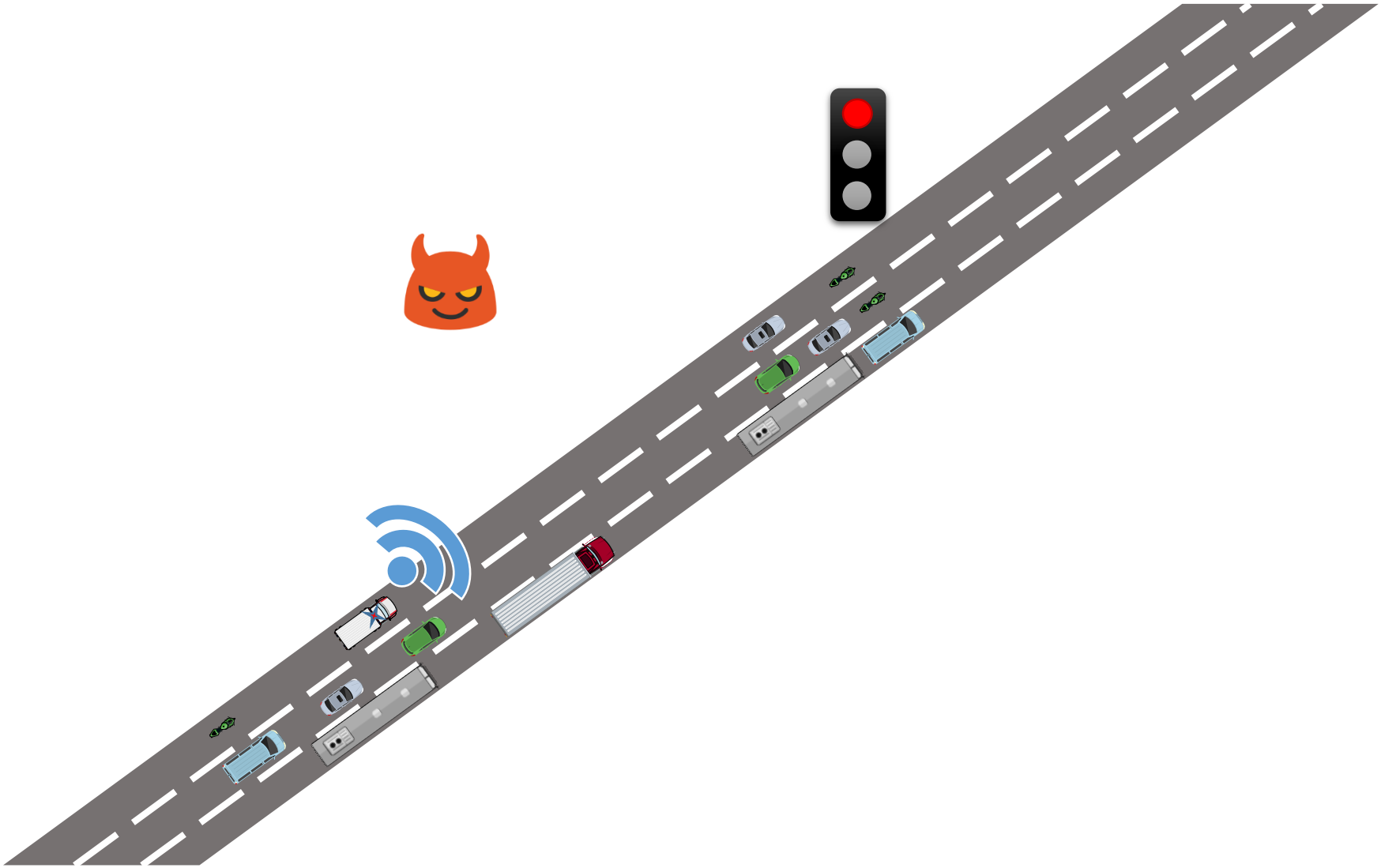


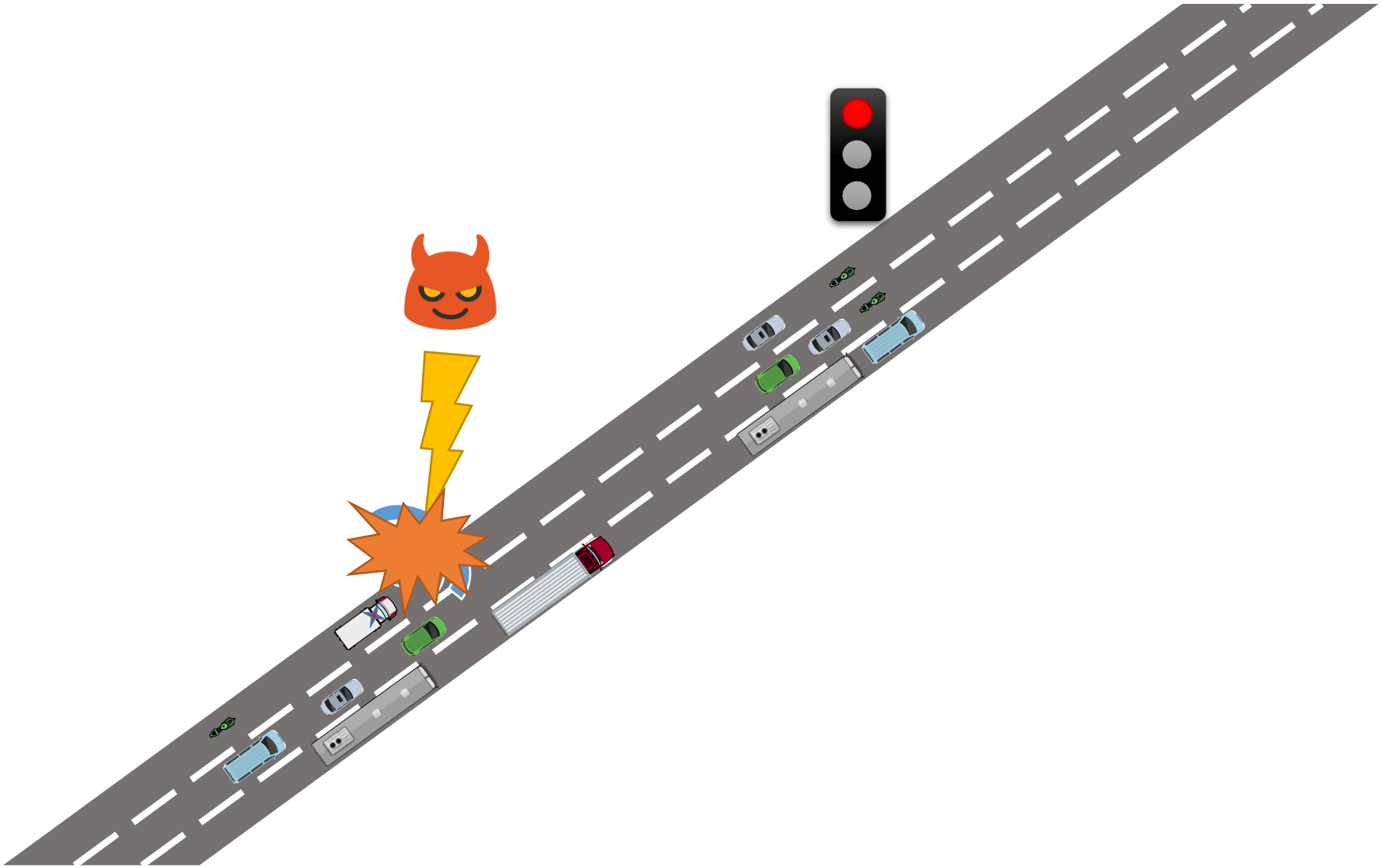


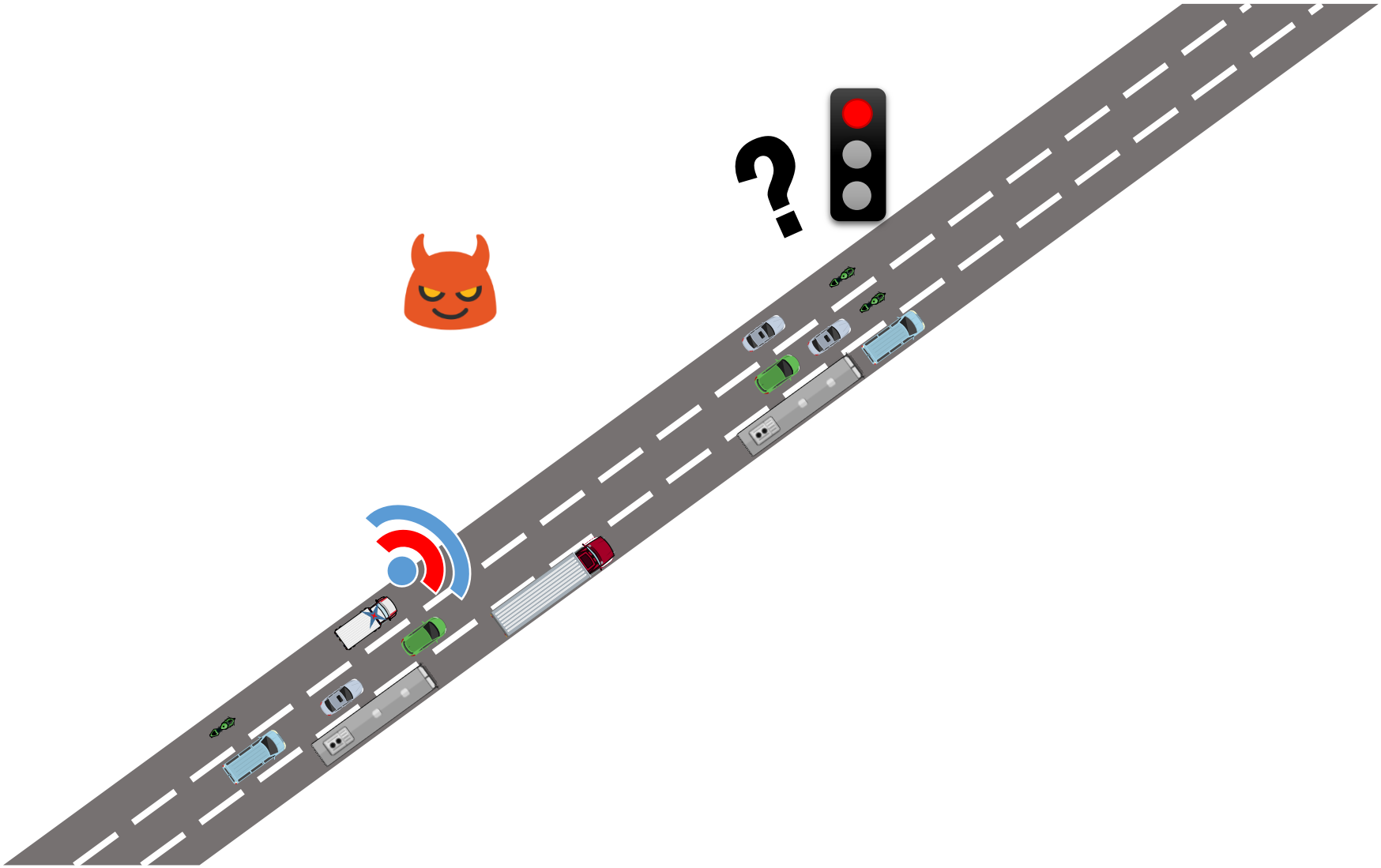


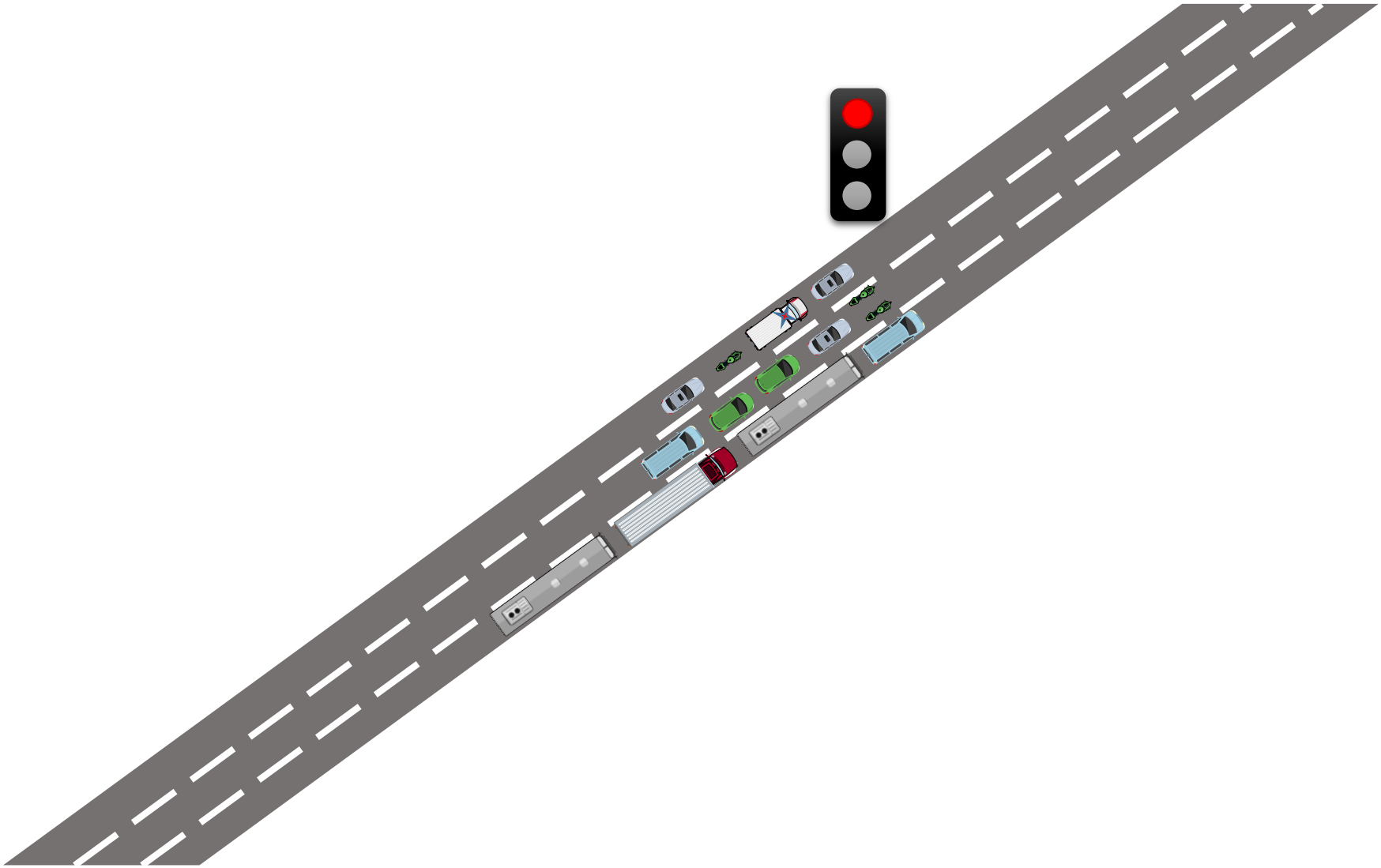
Integridad?

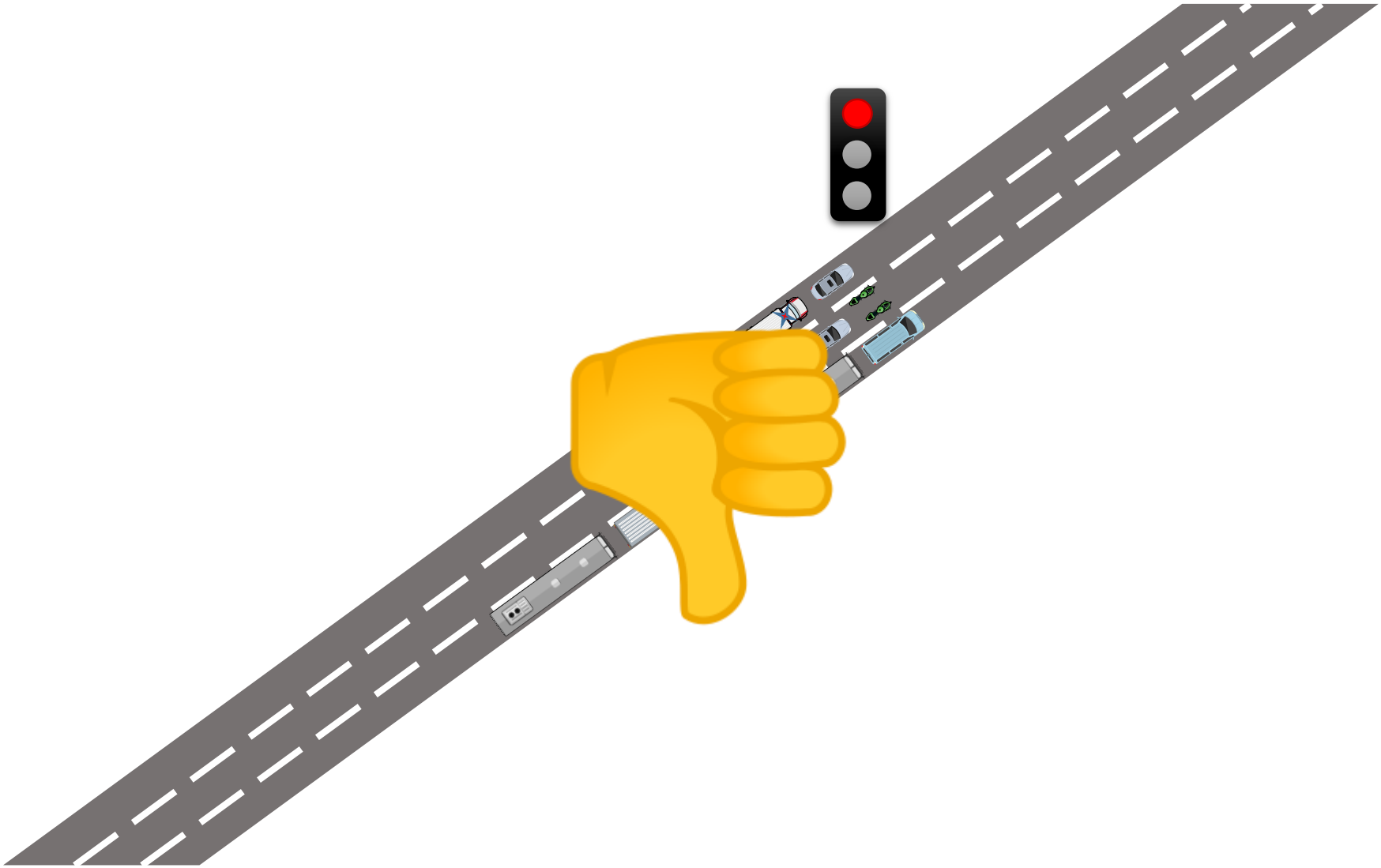




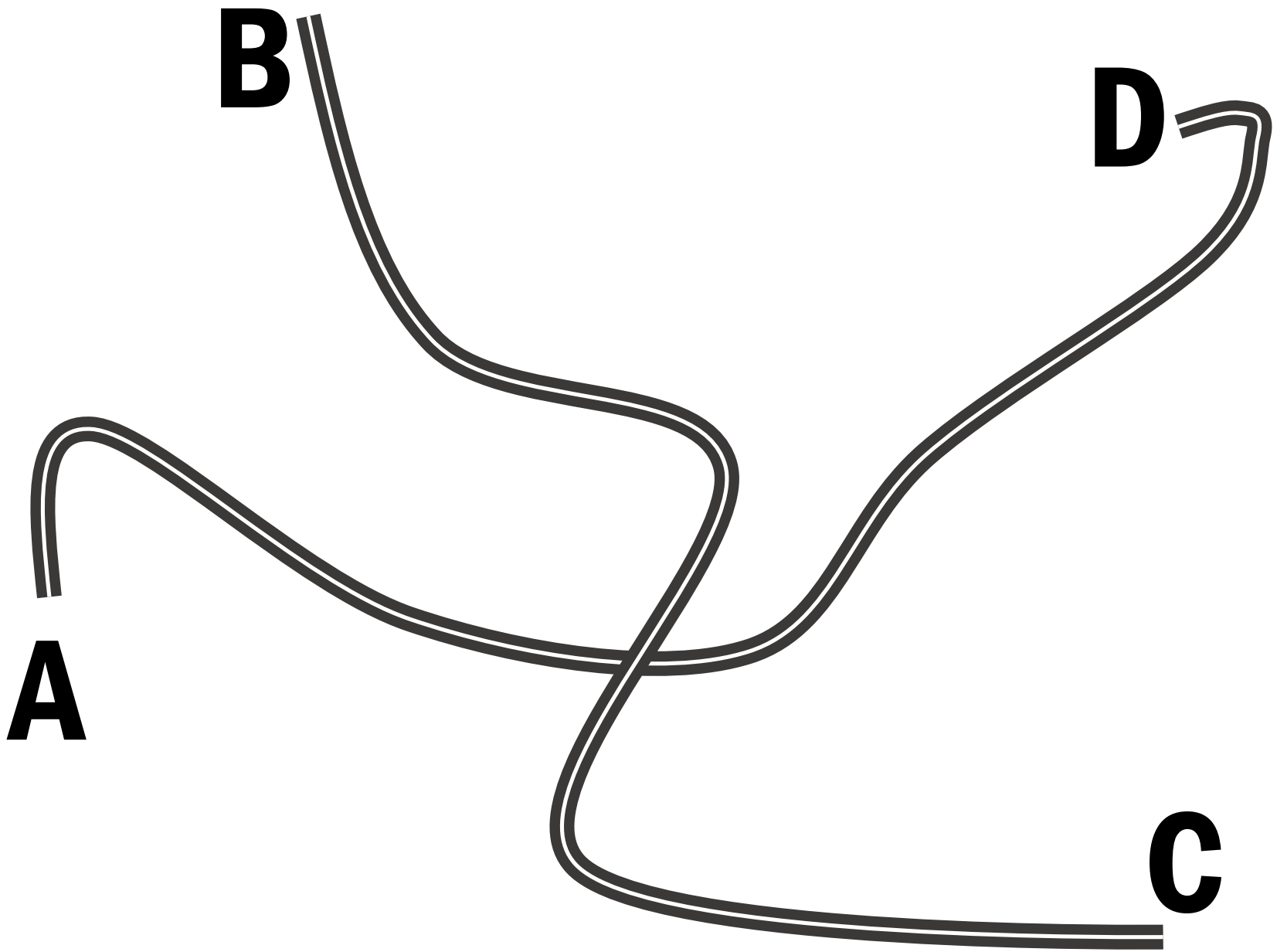


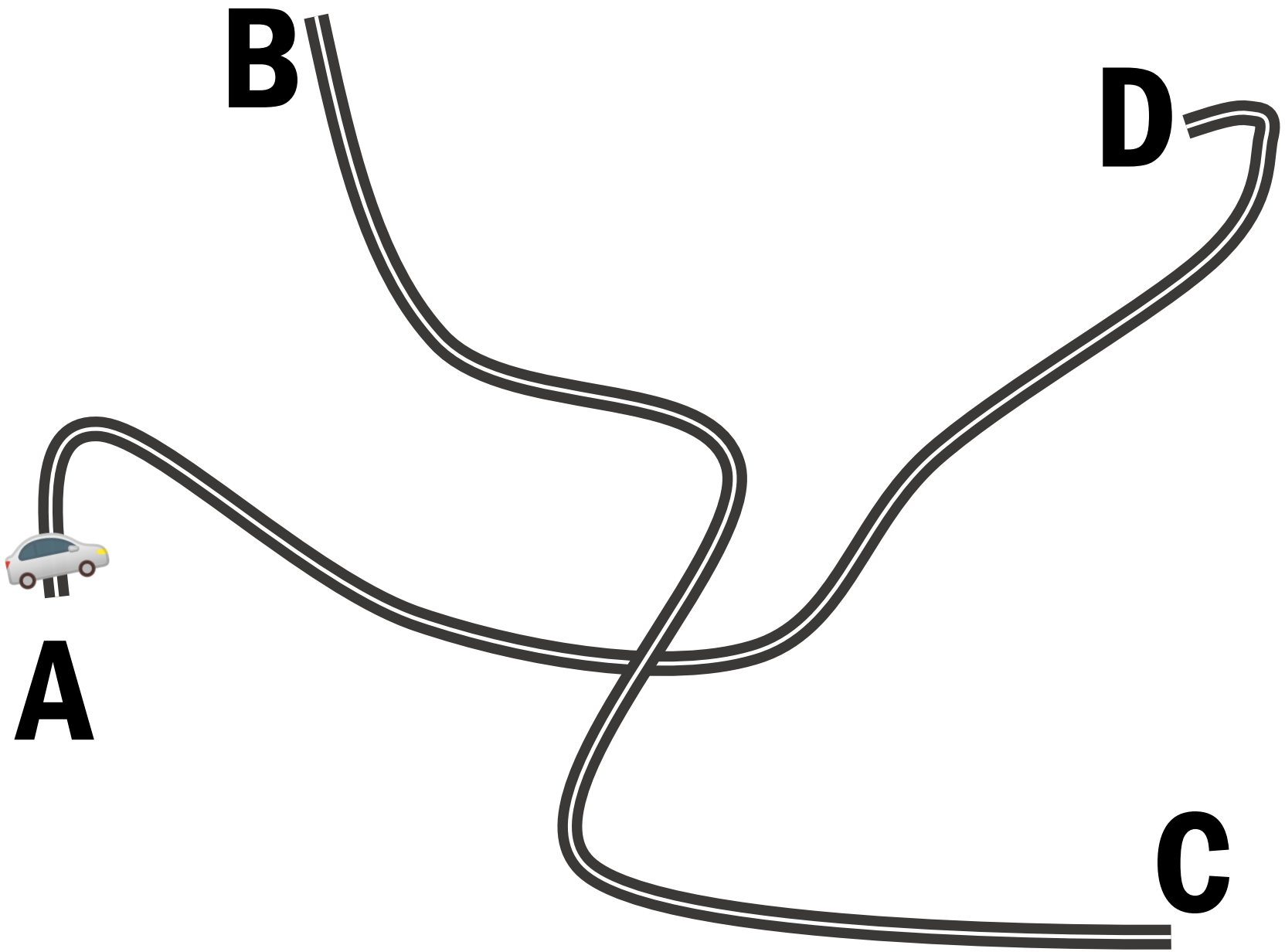


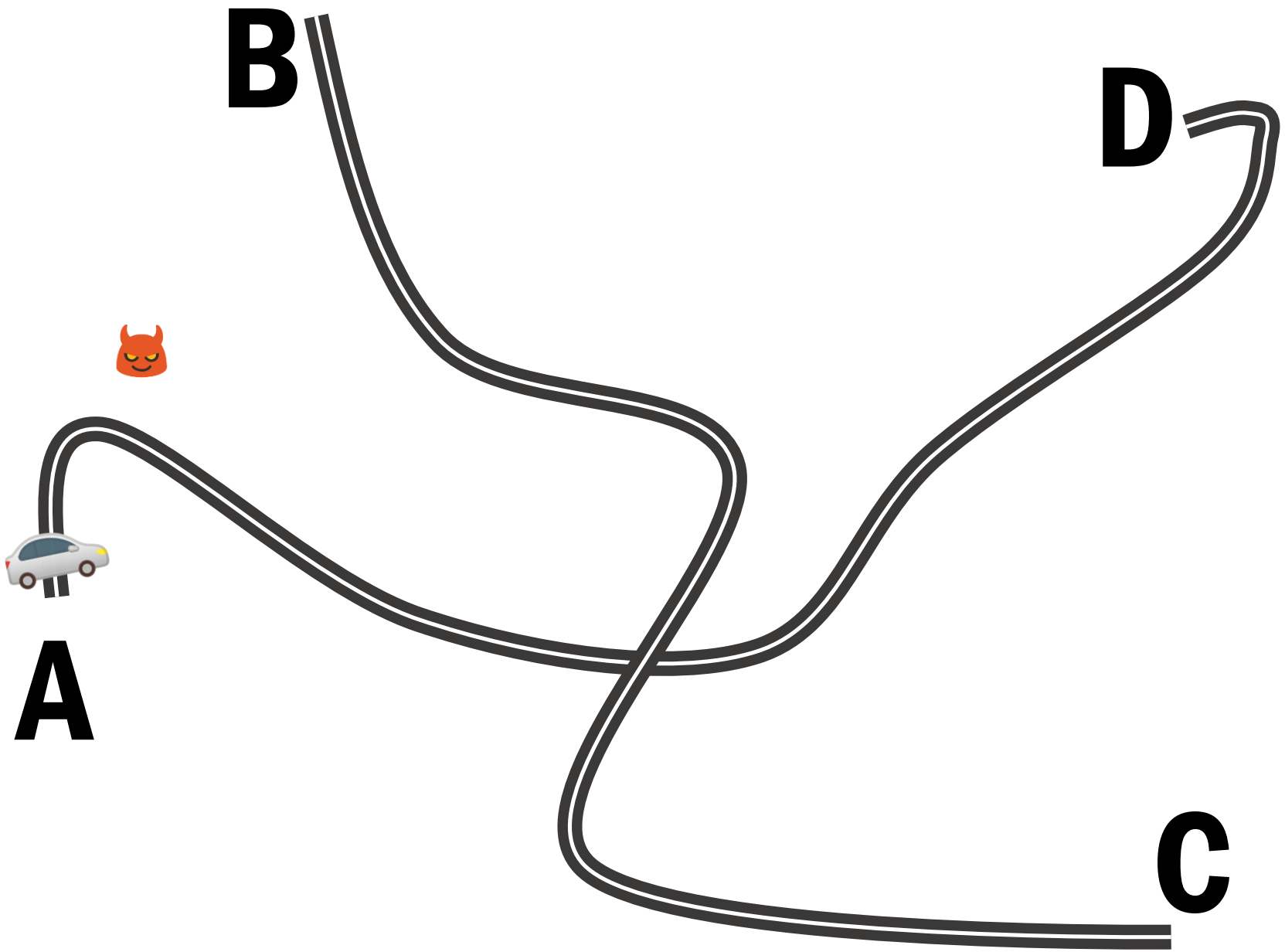


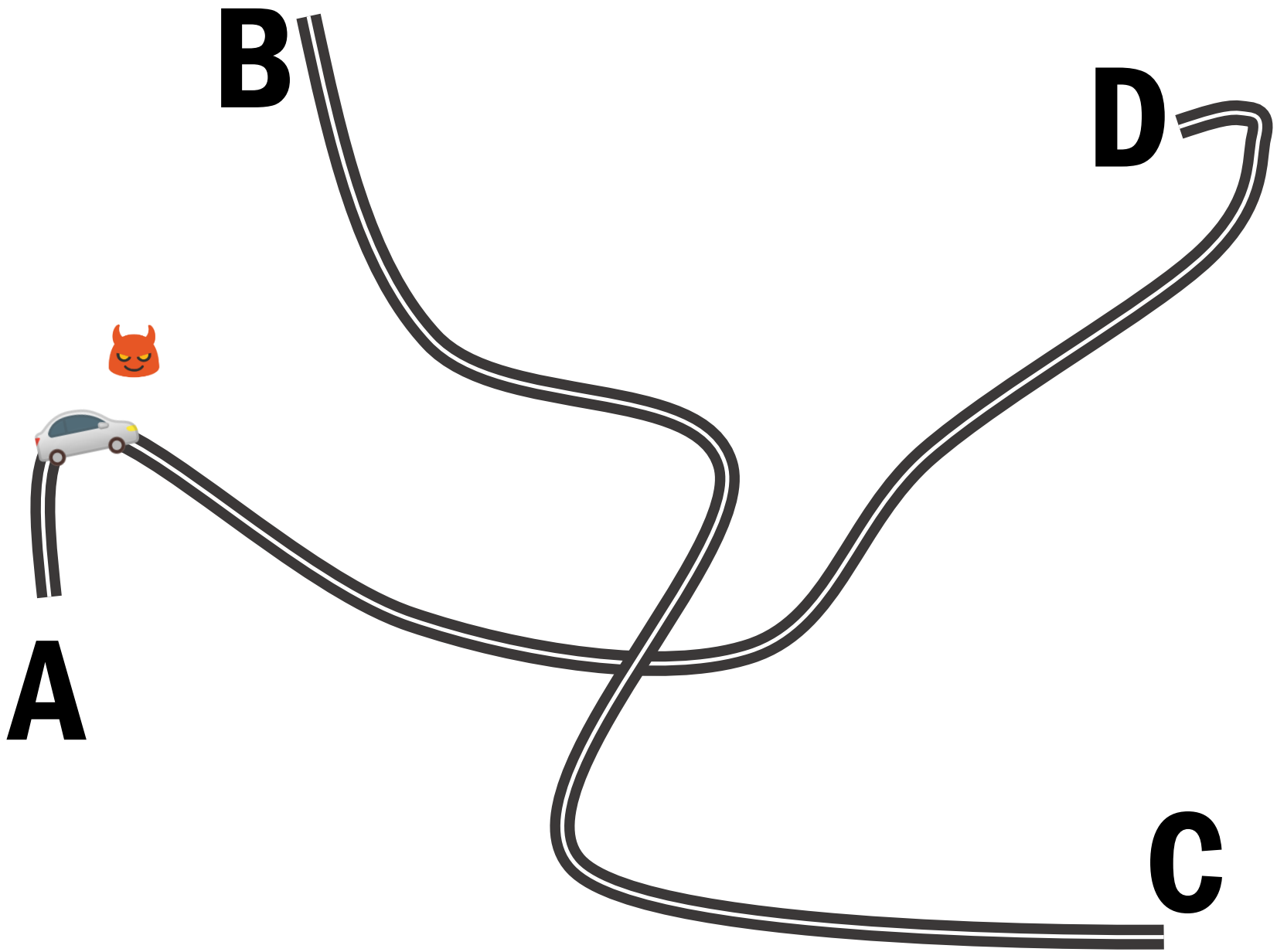


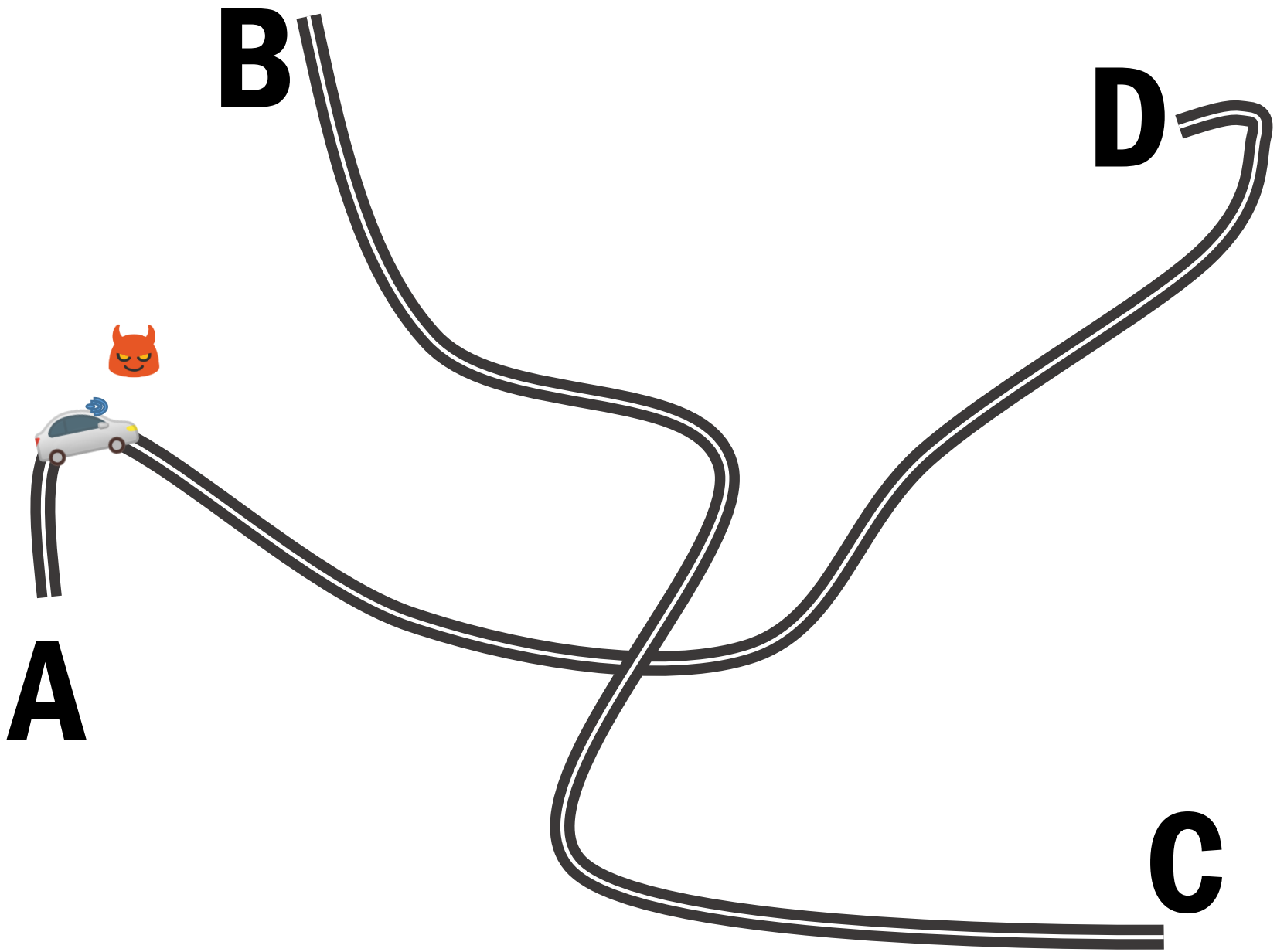
Privacidad?

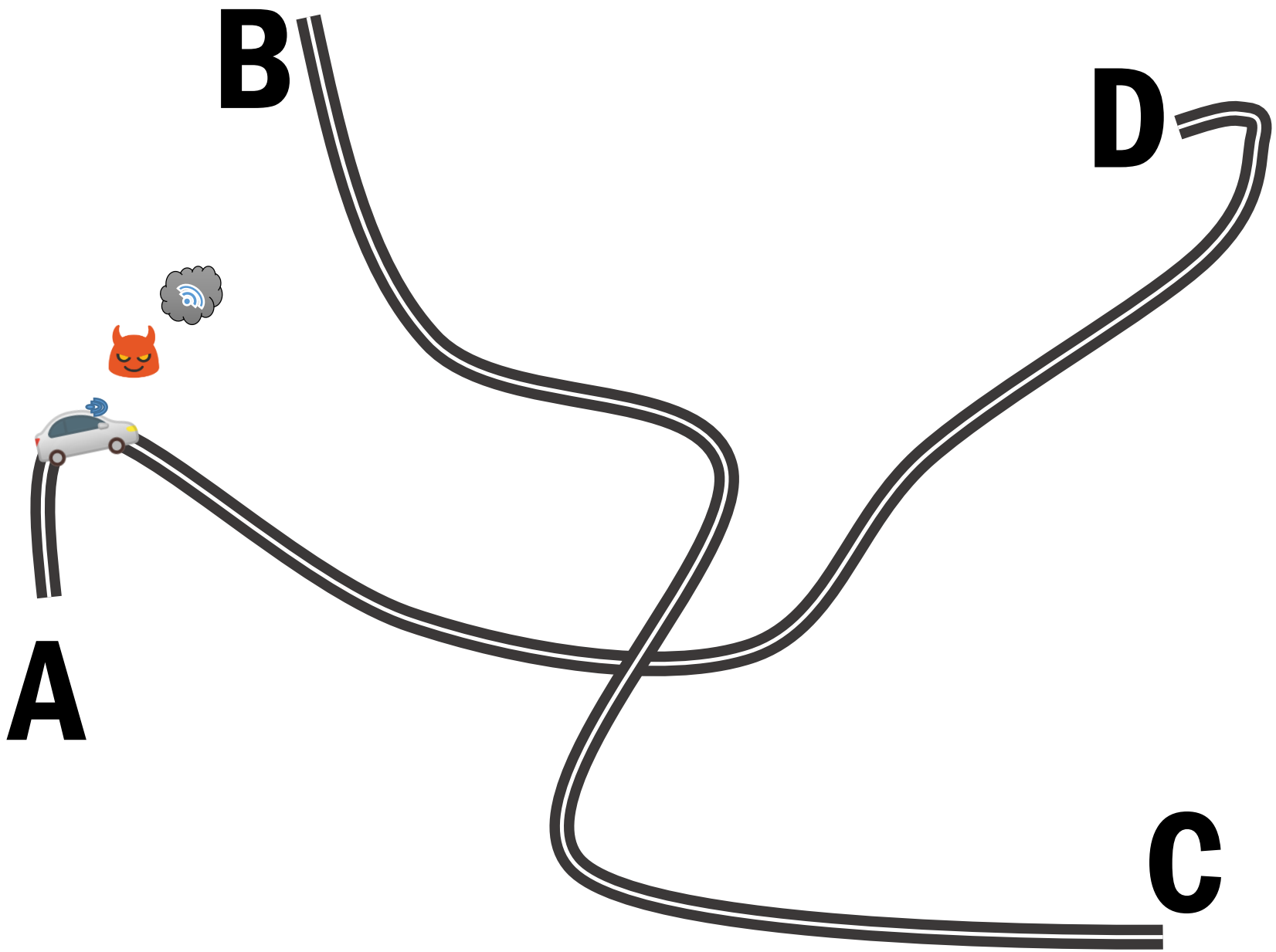

B
D
A
C

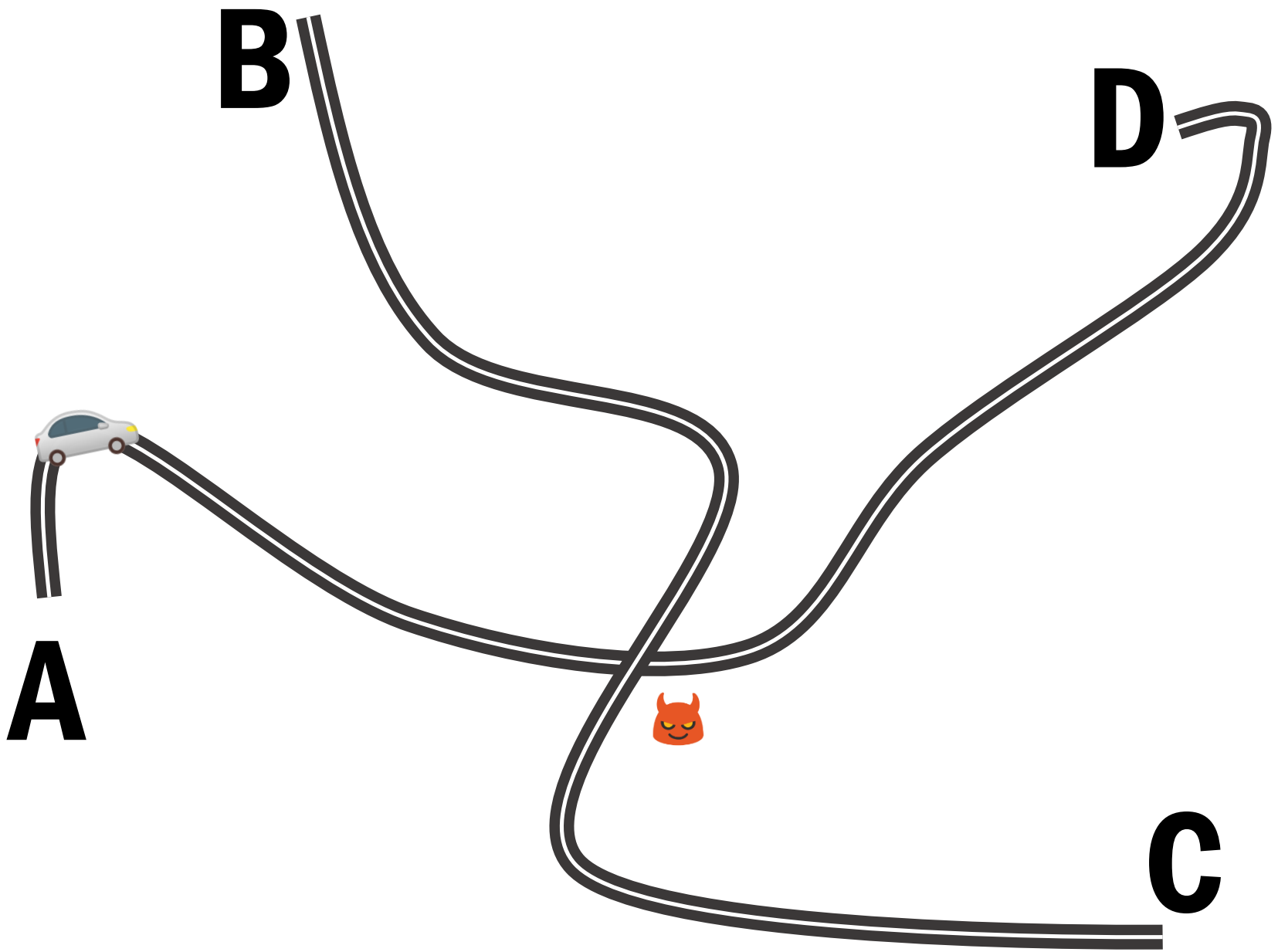

B
D
A
C

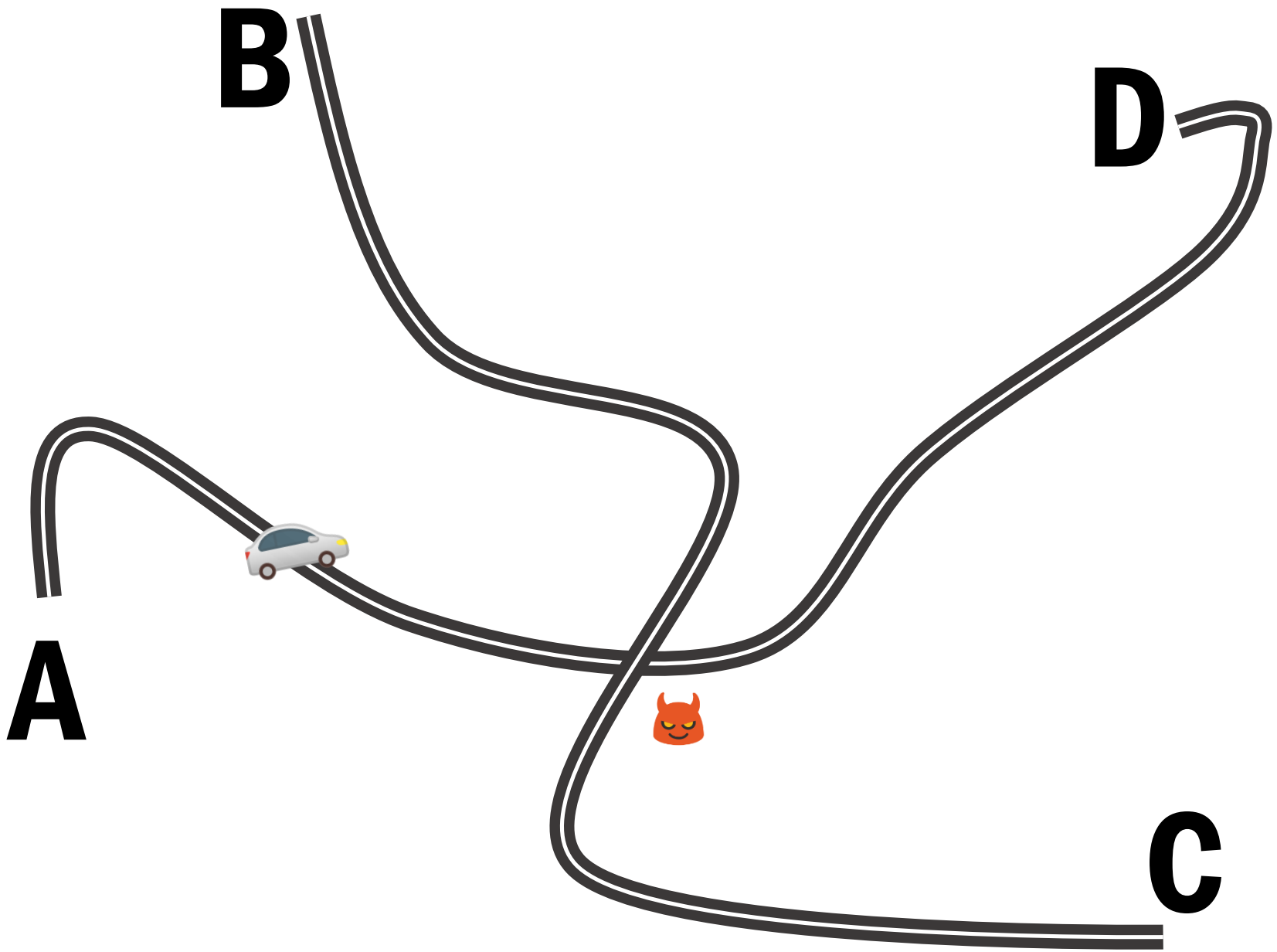

B
D
A
C

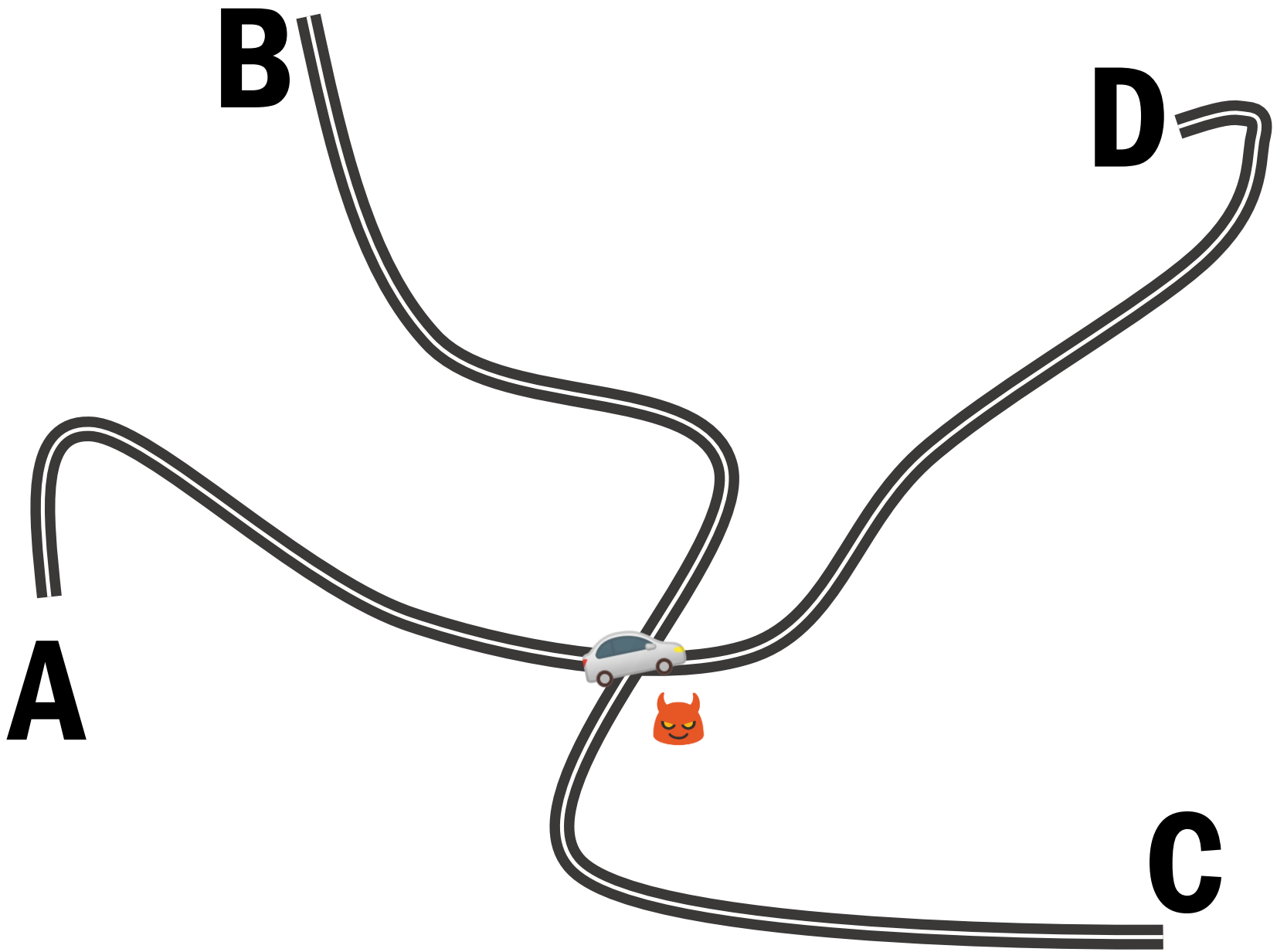

B
D
A
C

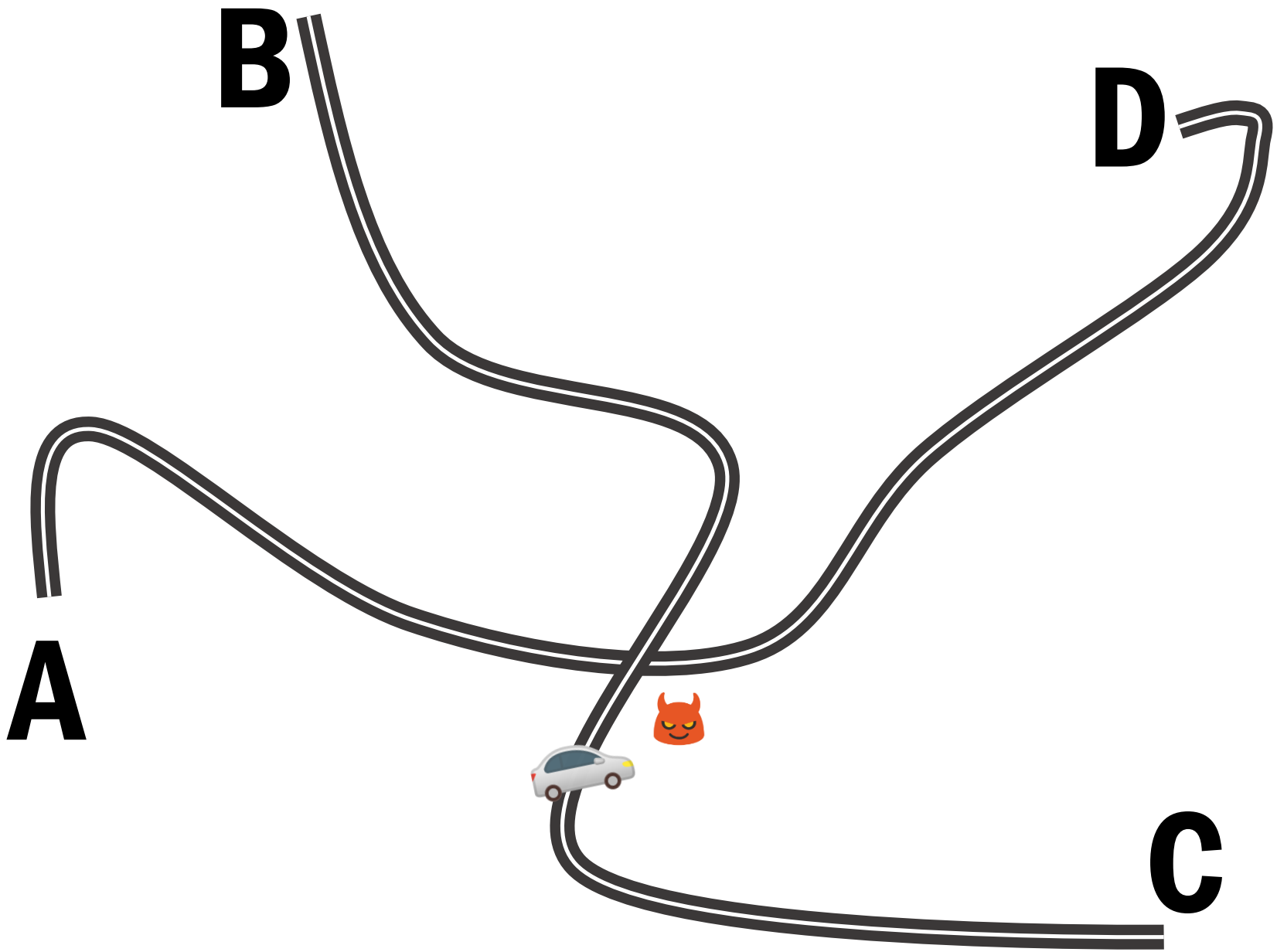

B
D
A
C

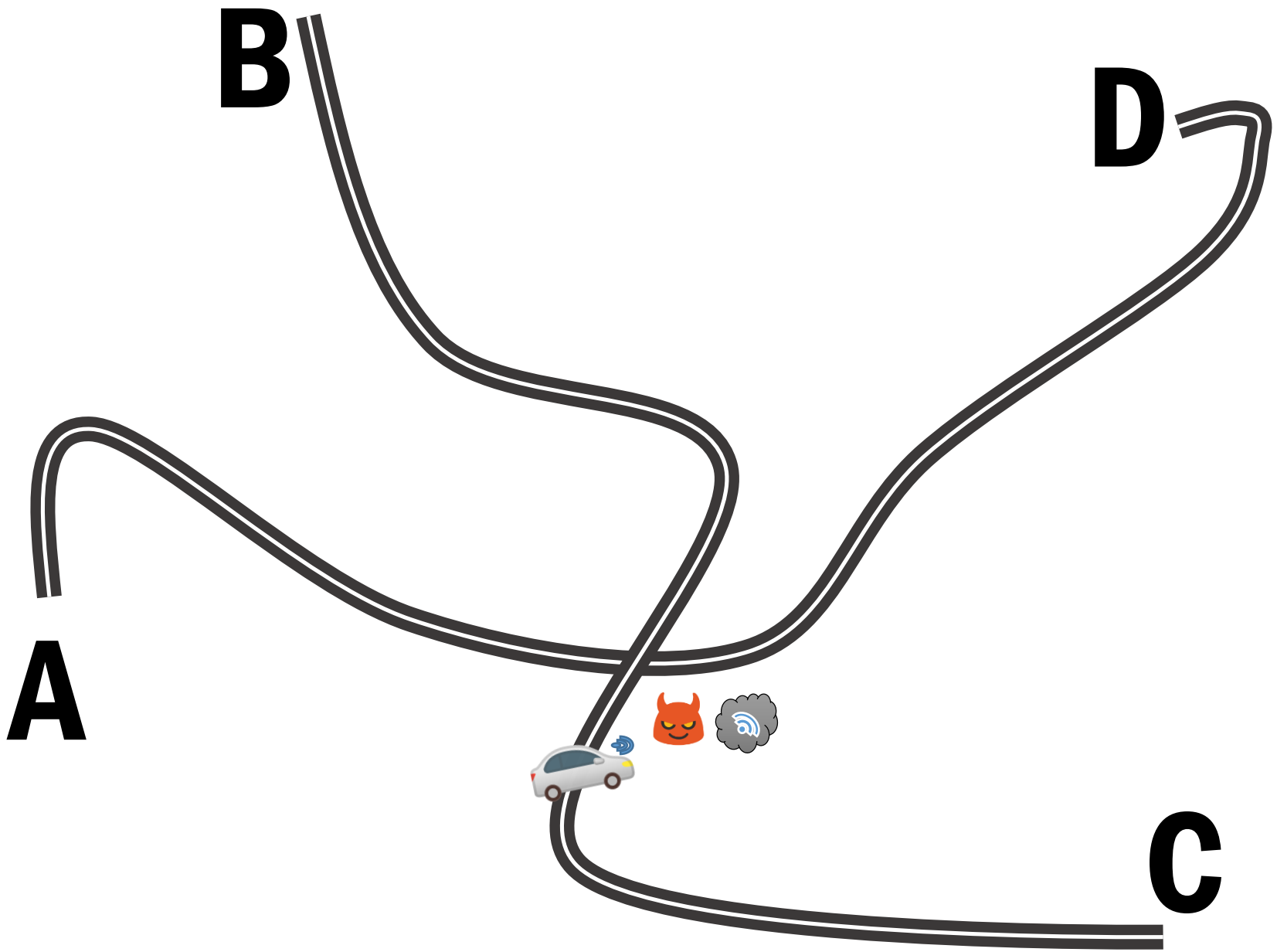

B
D
A
C


B
D
A
C


B
D
A
C


B
D
A
C


B
D
A
C


B
D
A
C

A → C

A → C

Public Key Infraestructure (PKI)

- Necesidad de establecer relaciones de confianza, es necesario tener identificadas y registradas tanto las estaciones de ITS como RSU's y OBU's.
  - Los certificados ayudan a crear esas relaciones de confianza.
- Para conseguir la privacidad de los vehículos se pueden usar certificados de pseudónimos.

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

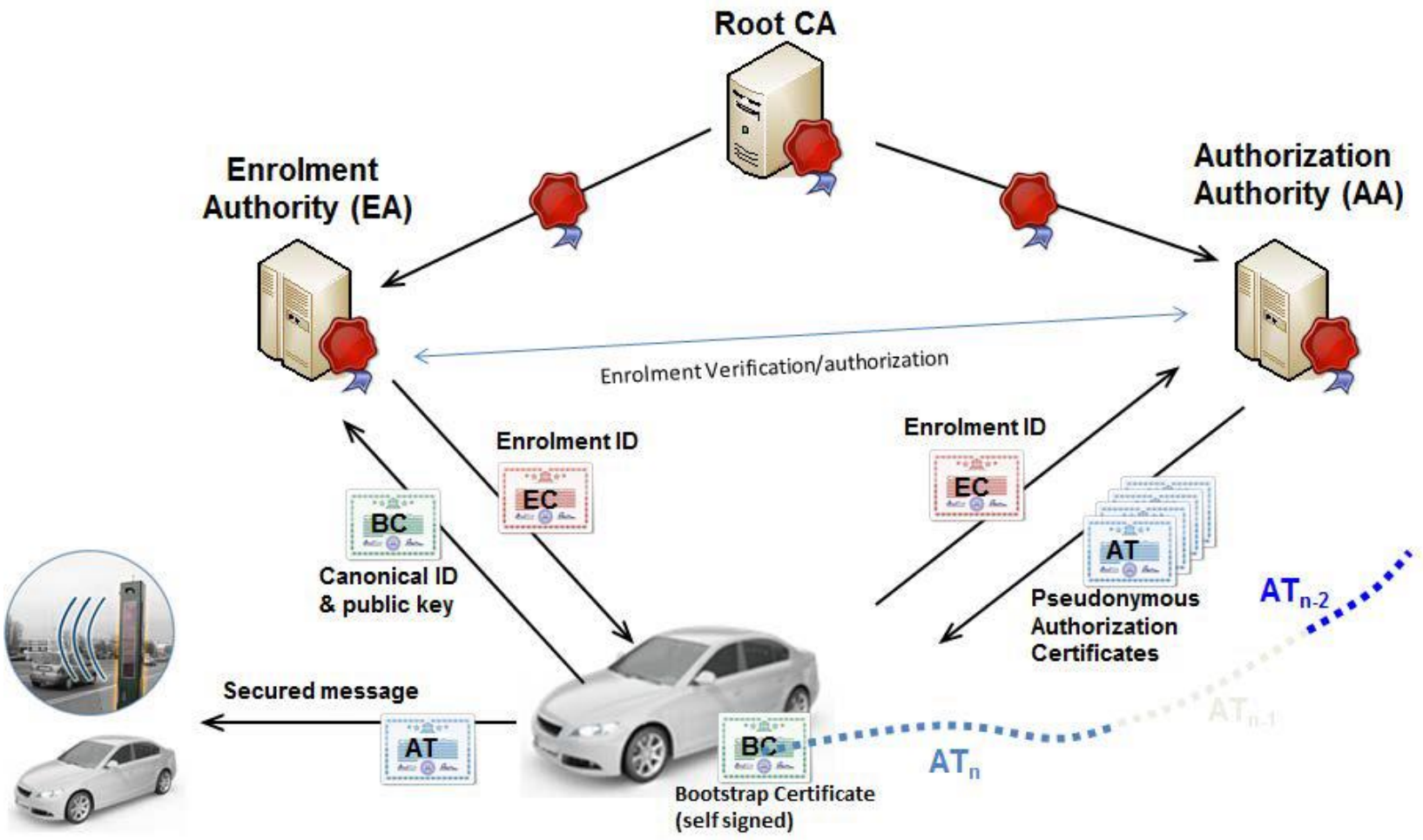
Estándares para implementar PKI

Specifications	Details
Governance	Security Policy & Governance Framework Release 1
Trust Model	Certificate Policy Release 1
Certificate Data Structure	ETSI TS 103 097 v.1.3.1
Cryptographic Algorithms	ETSI TS 103 097 v.1.3.1 (NIST and Brainpool) Certificate Policy v1.0
Download C-Roads CTL	ETSI TS 102 941 (v.1.2.1)
Download C-Roads CRL	ETSI TS 102 941 (v.1.2.1)
C-Roads CTL data structure	ETSI TS 102 941 (v.1.2.1)
C-Roads CRL data structure	ETSI TS 102 941 (v.1.2.1)
Verification Algorithm for Certificate/ Signature	Only for ETSI TS 103 097 v.1.2.1

Estándares para implementar PKI

- ETSI-TS 102 940 – ITS communications security architecture and security management.
- ETSI-TS 102 941 (v1.2.1) – Trust and Privacy Management (borrador)
- ETSI-TS 103 097 (v1.3.1)– Security header and certificate formats.

Arquitectura y funcionamiento

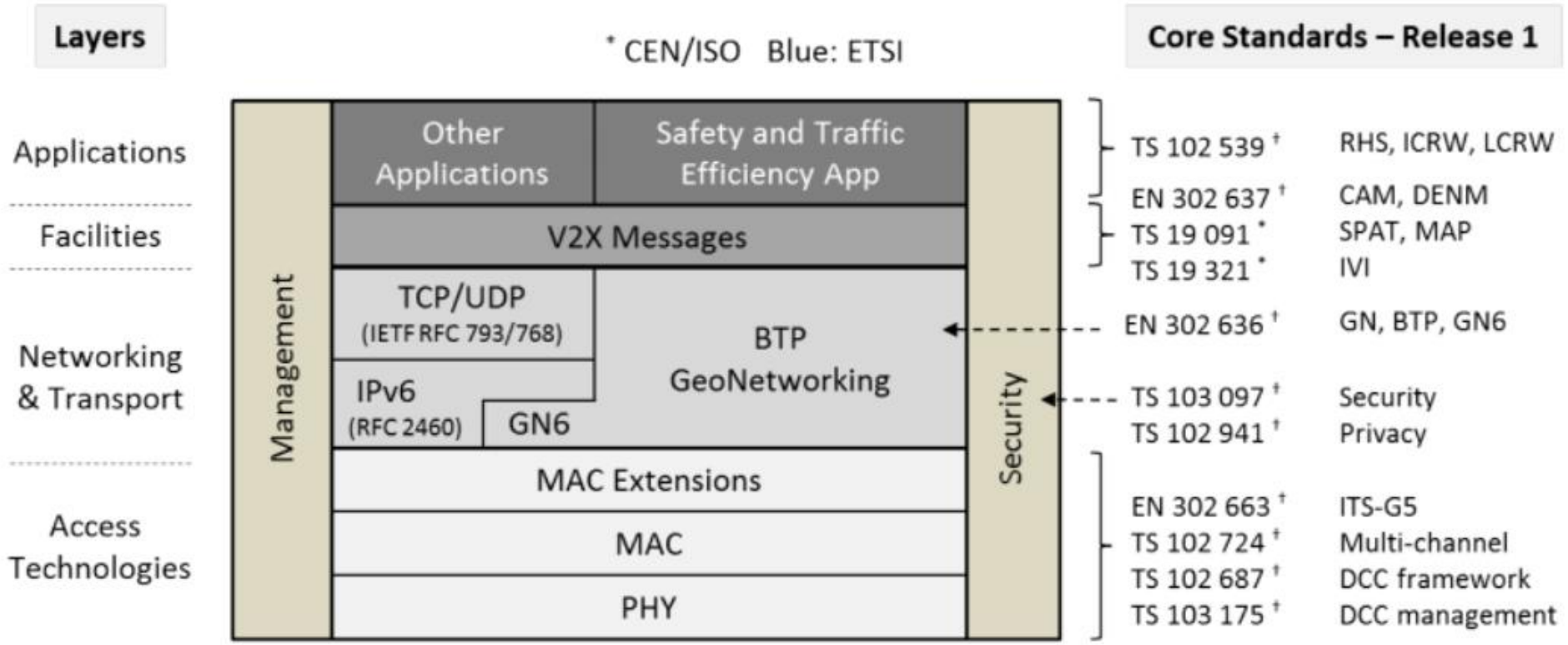


Ciclo de vida de la seguridad

- Fabricar :
  - Se usará métodos físicos seguros para la generación de los datos en este proceso (TPM).
  - Identificador canónico que es globalmente único
  - Información de contacto para EA y AA
  - Dirección de red
  - Conjunto de certificados confiables de EA's.
  - Conjunto de certificados confiables de AA's.
  - Un par de claves pública / privada para fines criptográficos.

- Registrar:
  - El ITS-S solicita su certificado de inscripción/registro al EA.
- Autorizar:
  - El ITS-S solicita su/s certificado/s de autorización al AA.
- Mantener:
  - Gestión de bajas (Listas de revocación) y altas de EA y AA.

Pila G5


Layers
* CEN/ISO Blue: ETSI
Core Standards – Release 1
Applications
Facilities
Networking & Transport
Access Technologies
Management
Other Applications
Safety and Traffic Efficiency App
V2X Messages
TCP/UDP (IETF RFC 793/768)
IPv6 (RFC 2460)
GN6
BTP GeoNetworking
MAC Extensions
MAC
PHY
Security
TS 102 539 † RHS, ICRW, LCRW
EN 302 637 † CAM, DENM
TS 19 091 * SPAT, MAP
TS 19 321 * IVI
EN 302 636 † GN, BTP, GN6
TS 103 097 † Security
TS 102 941 † Privacy
EN 302 663 † ITS-G5
TS 102 724 † Multi-channel
TS 102 687 † DCC framework
TS 103 175 † DCC management

Mensajes ITS

Sin seguridad:

MAC Header	LLC Header	Basic Header	Common Header	Extender Header	Payload

Añadiendo seguridad:

MAC Header	LLC Header	Basic Header	**Secure Header**	Common Header	Extender Header	Payload	**Secure Trailer**

¿Preguntas?

- antonio.rodriguez.g@escert.upc.edu
- https://twitter.com/tonrodriguez_
- https://twitter.com/escert_upc
- https://inlab.fib.upc.edu/es/persones/antonio-rodriguez

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

inLab FIB talent & tech