ROGUE ROBOTS AND THE POTENTIAL FOR CYBER ATTACK

#roguerobots

Mark Nunnikhoven @marknca

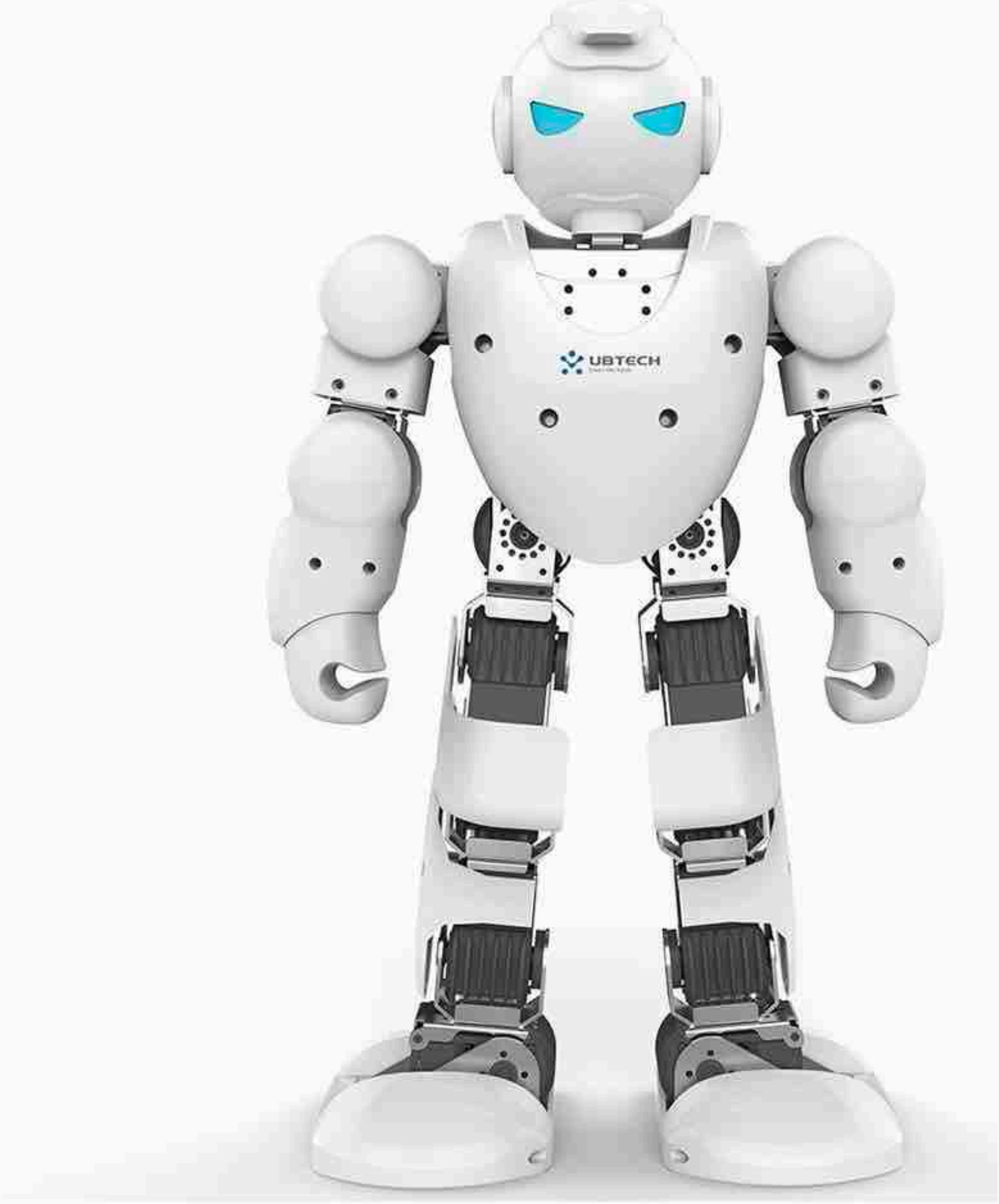
SXSW®

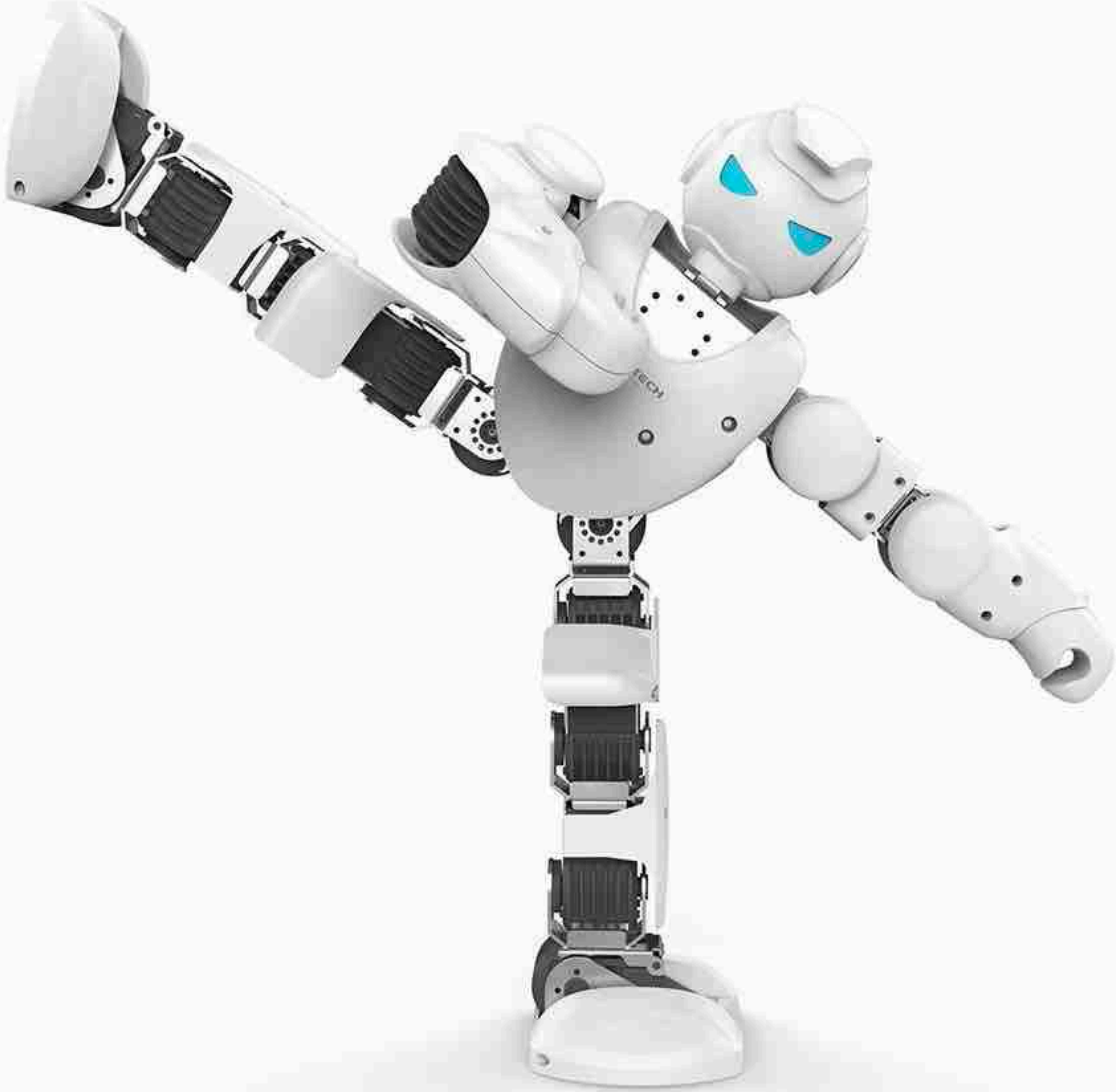
Originally presented at SXSW 2018 on Monday, 12-Mar-2018

1963 →

GOLD KEY
THE JETSONS
The JE
10041-403
MARCH
by HANNA-BAR
© 1964, HANNA-BARBERA PRODUCTIONS, INC.
DC
THE Jetsons
Hanna-Barbera
1
PALMIOTTI
BRITO

← 2017





UBTECH
Dream With Robots

DOCK
CLOCK
SCHEDULE
SPOT

Skydio

RISK

The goal of cybersecurity

Make sure that systems work as intended

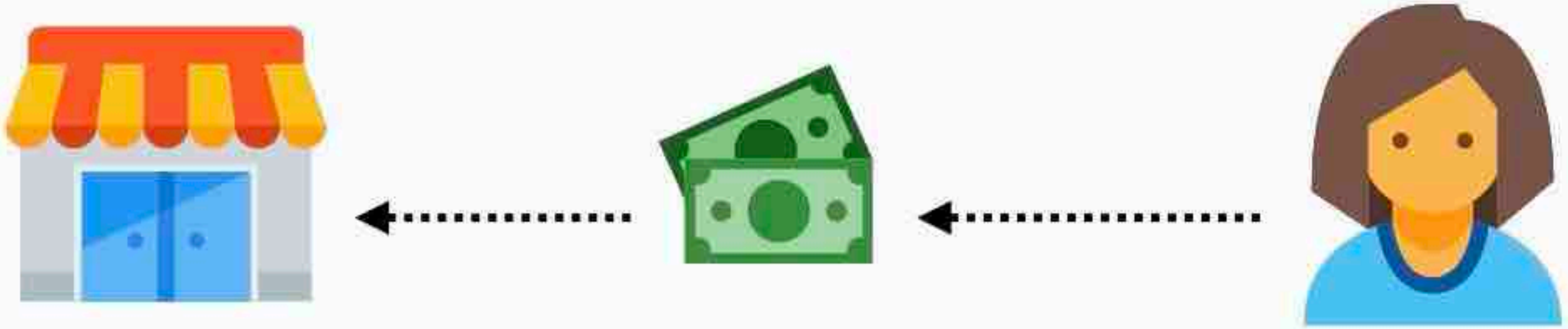
The goal of cybersecurity

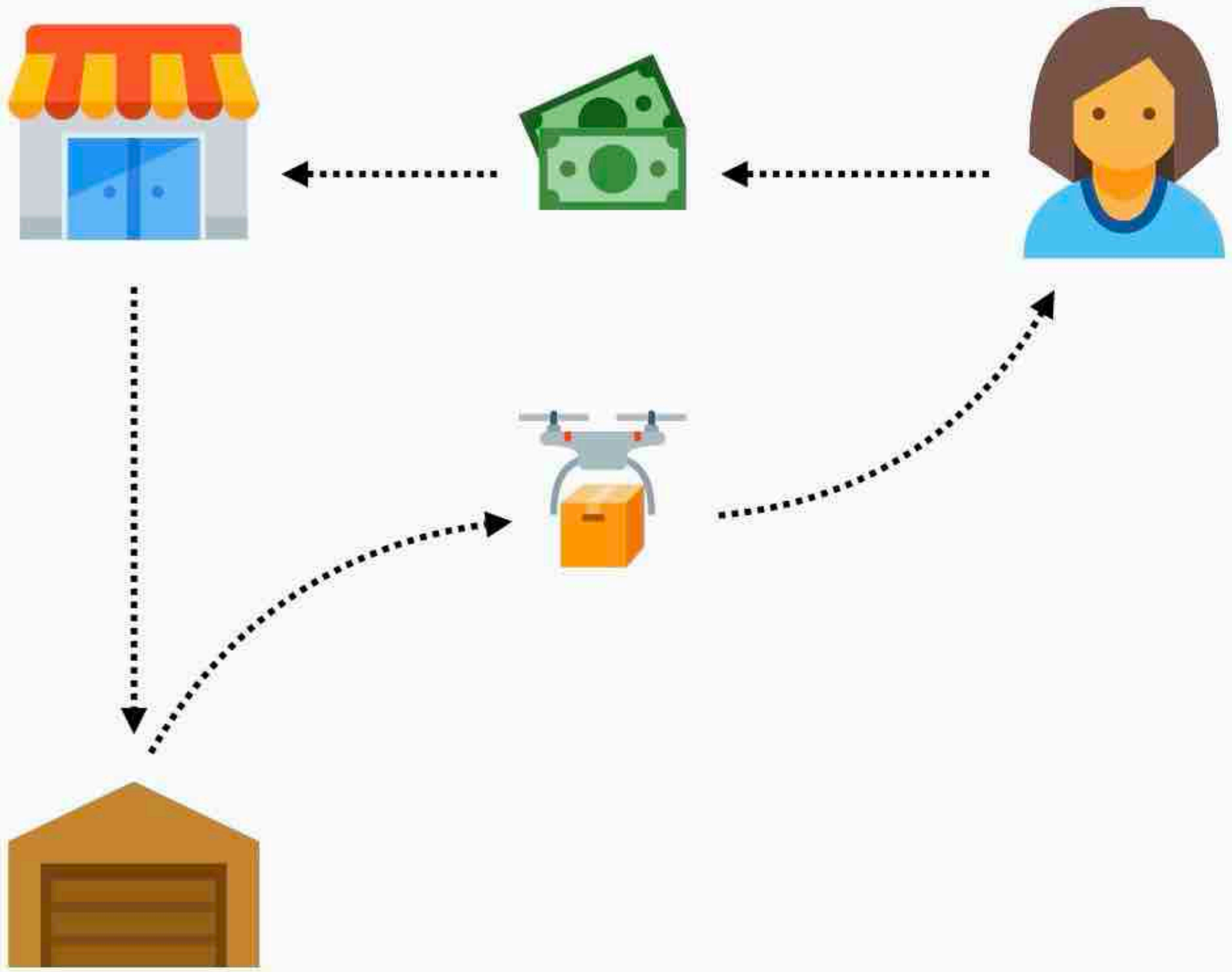
Make sure that systems work as intended ...and ONLY as intended

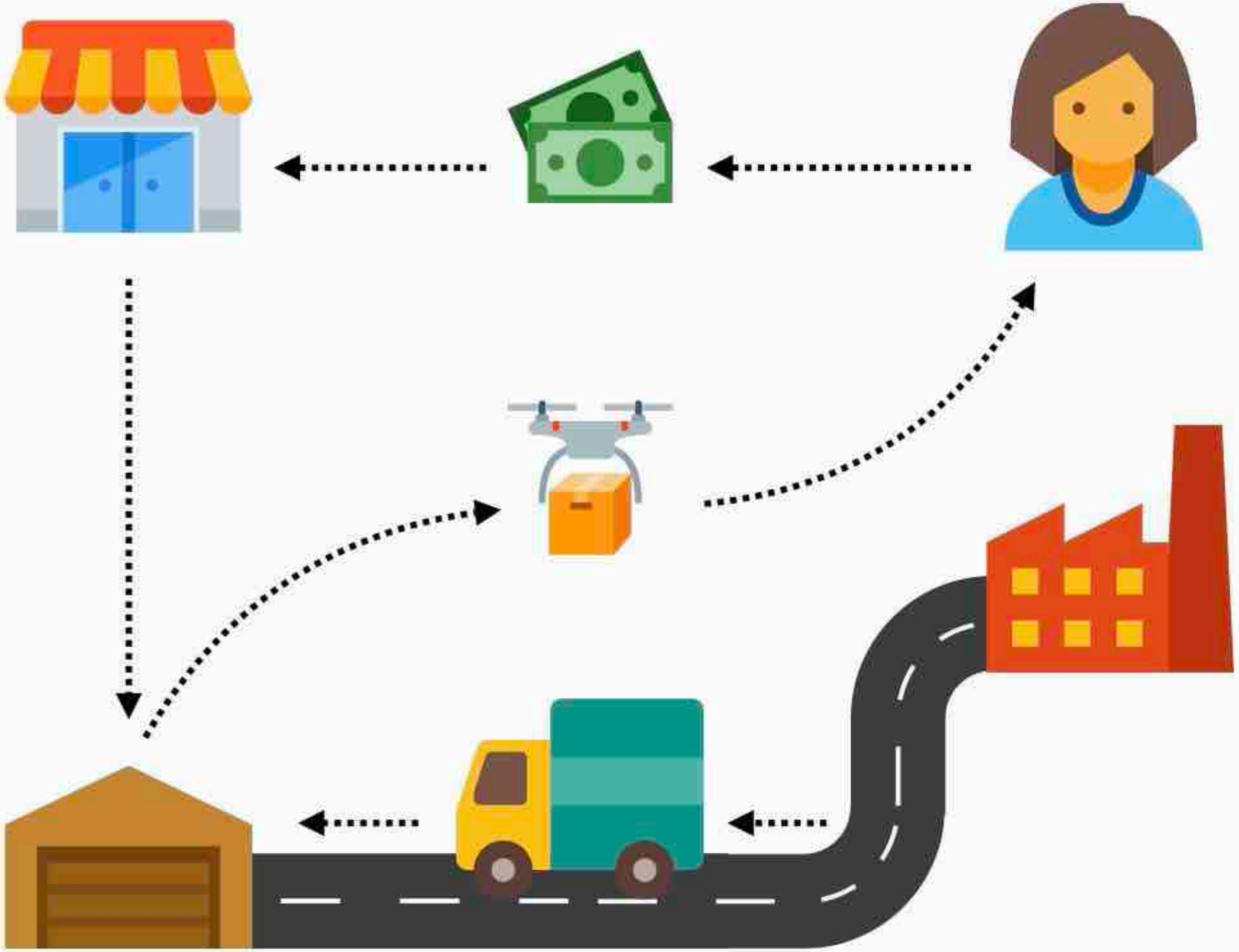
KB 46279860
100
HUNDRED DOLLARS

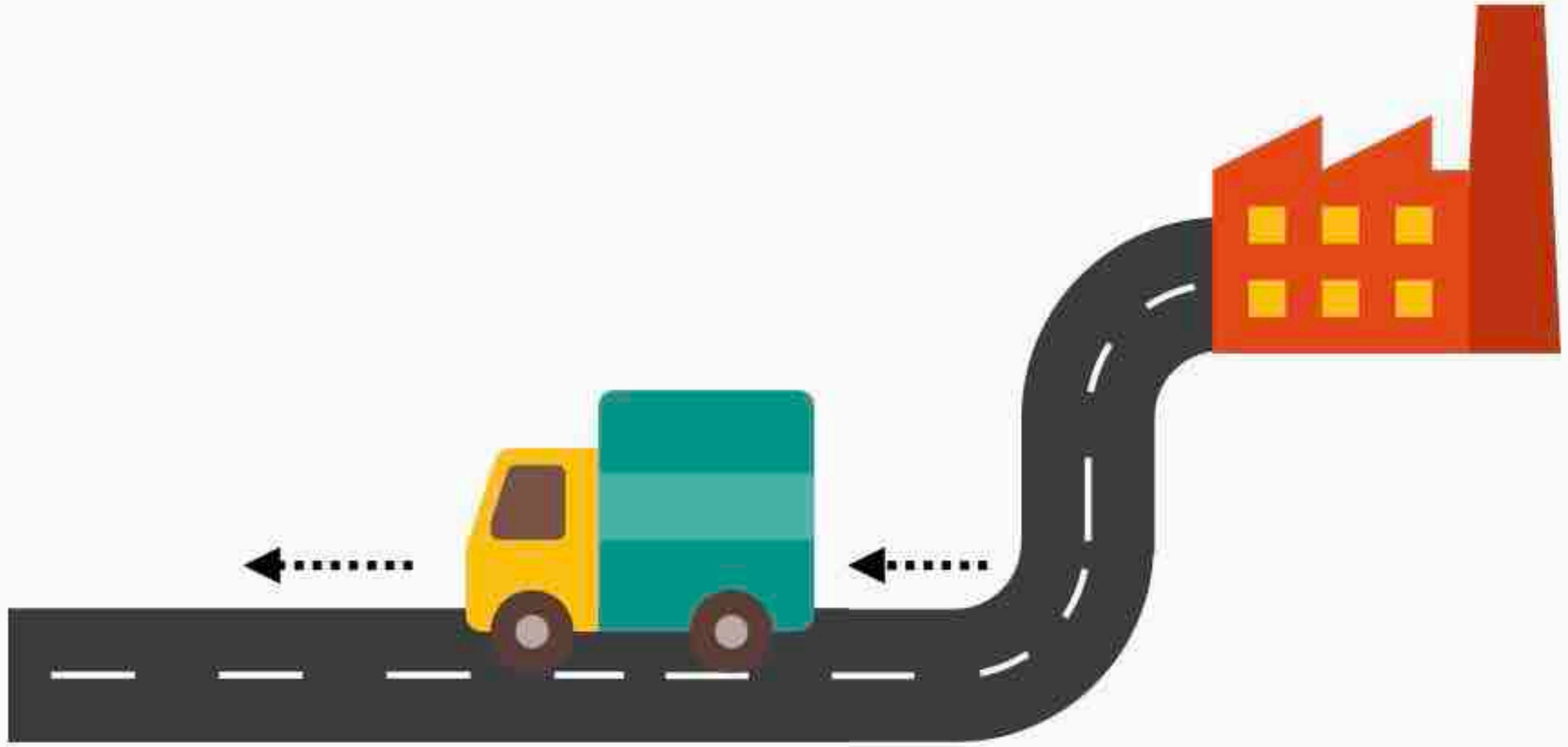
amazon
PrimeAi

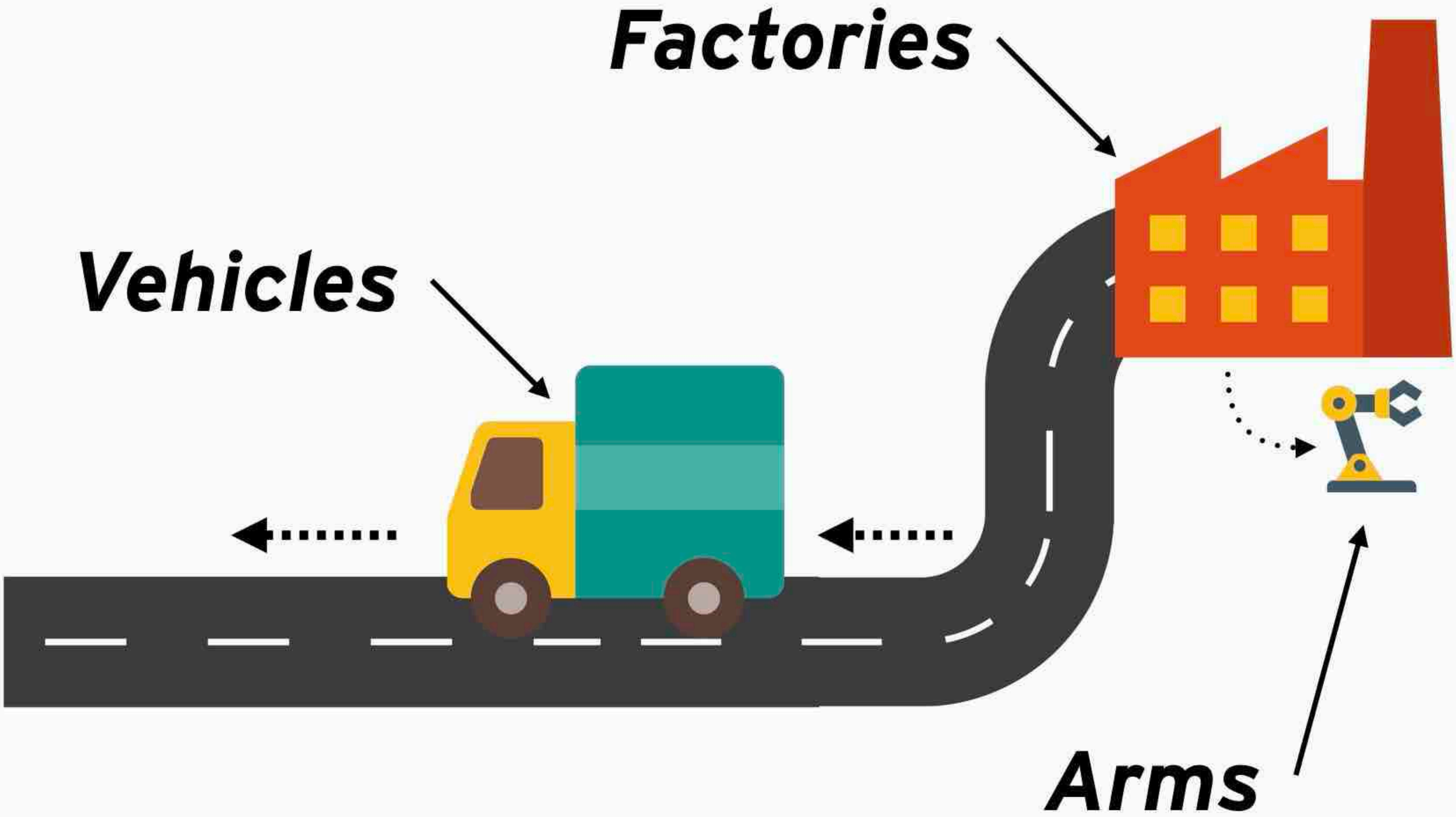
1B↑
2B↑
3B↑
4B↑
1A↑
2A↑
3A↑
4A↑
KIVA Systems
2178
KIVA Systems
1348
1348
1374
1375
1377











Factories

Vehicles

Arms

VEHICLES

9y

THE VERGE
TECH
SCIENCE
CULTURE
CARS
REVIEWS
LONGFORM
VIDEO
MORE
TRANSPORTATION
UBER
RIDE-SHARING
8
SHARE
NOW TRENDING

Uber's self-driving trucks are now delivering freight in Arizona

Via Uber Freight, the company's standalone trucking app

By Andrew J. Hawkins | @andyjayhawk | Mar 6, 2018, 10:00am EST

Self-driving truck and truck driver connect with Uber Freight

Fortnite Battle Royale is coming to iOS and Android

POPULAR SCIENCE

WANT MORE?

SCIENCE | TECH | DIY | GOODS | VIDEO | ROLL THE DICE | SUBSCRIBE

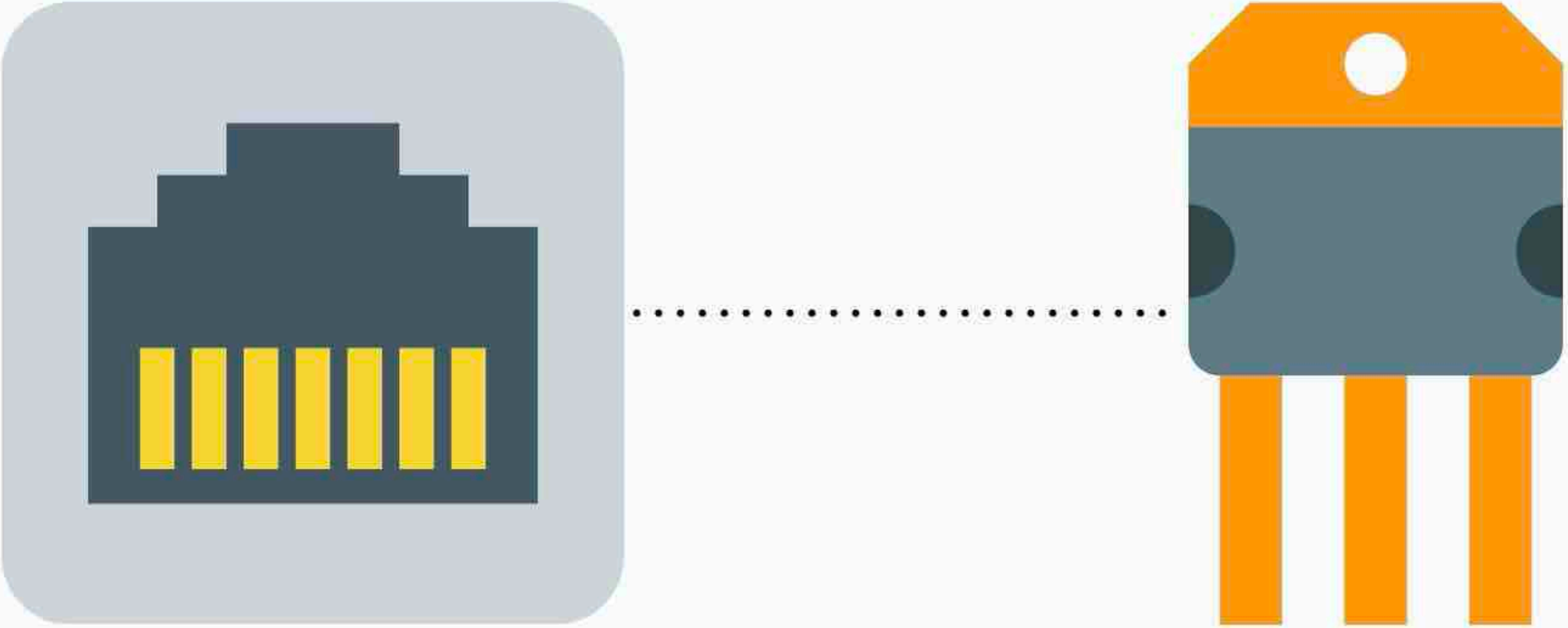
CARS

Robot Truck Convoy Tested In Nevada

Optimus Prime came home and got a day job.

By Kelsey D. Atherton *June 2, 2014*

GPS
00000



CAN Bus

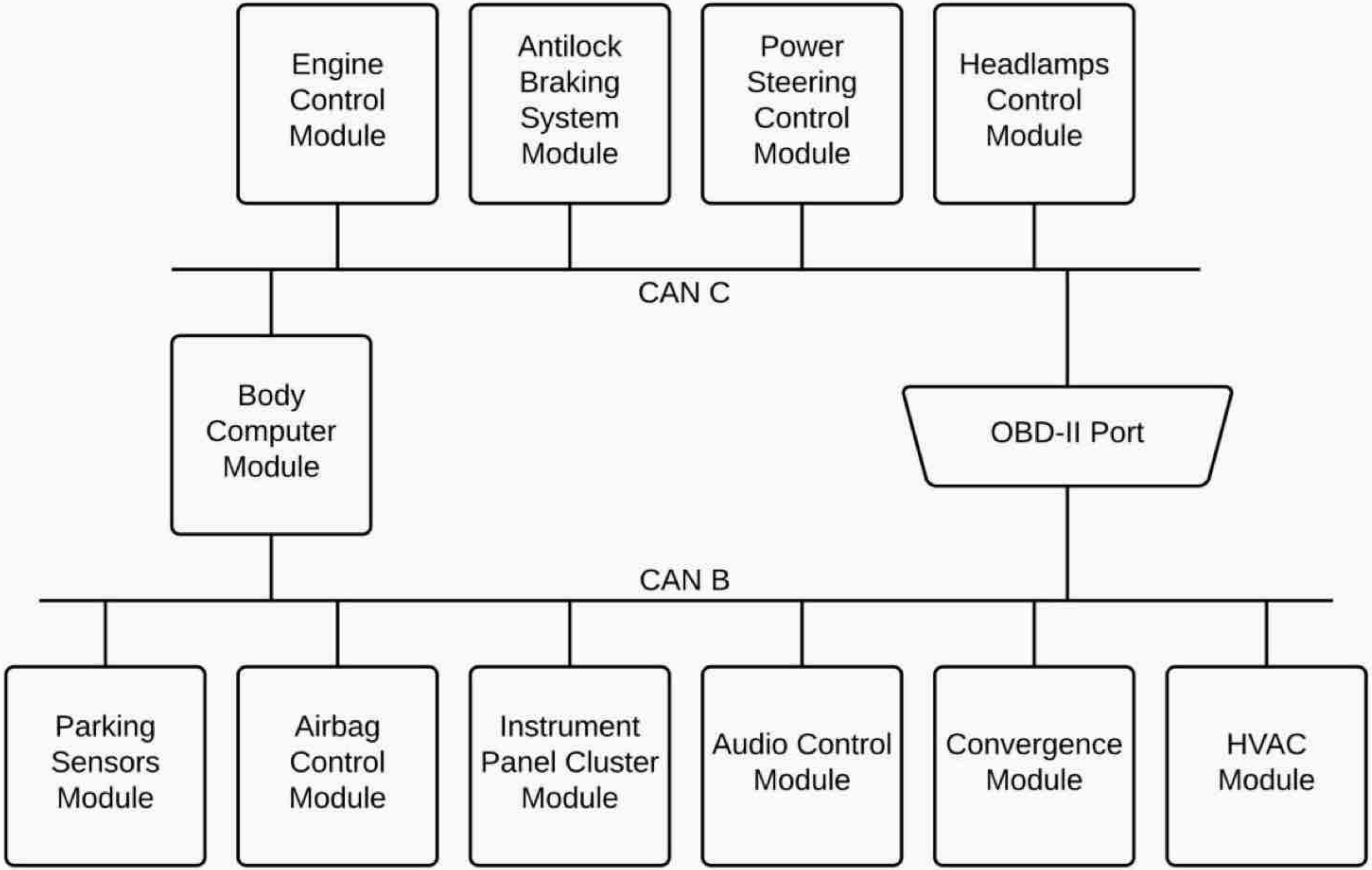
Controller Area Network

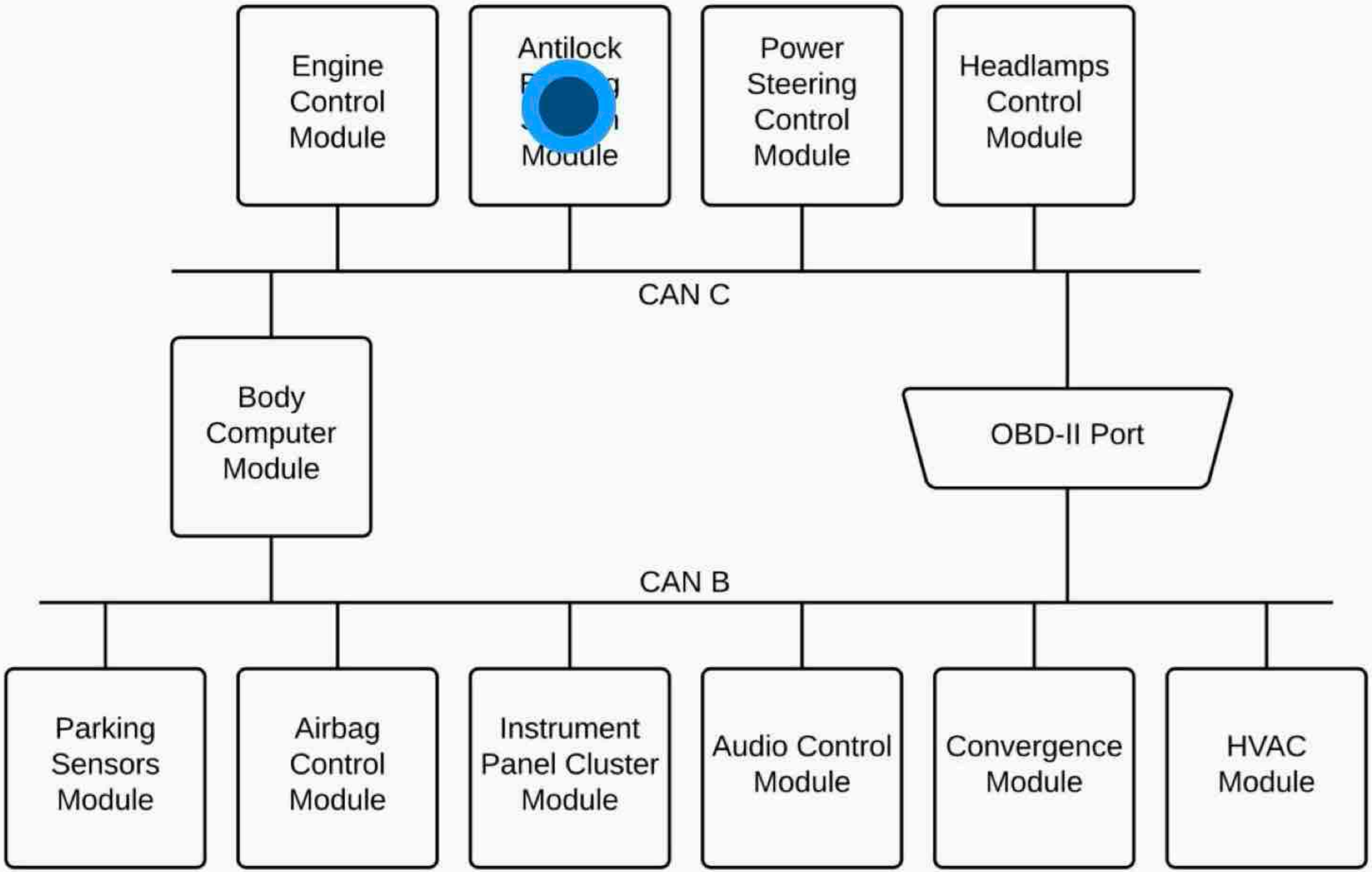
1986

Set as standard

** ISO 11898-*. Mandatory in North American consumer vehicle, all EU vehicles*

GPS
00000


Engine Control Module
Antilock Braking System Module
Power Steering Control Module
Headlamps Control Module
CAN C
Body Computer Module
OBD-II Port
CAN B
Parking Sensors Module
Airbag Control Module
Instrument Panel Cluster Module
Audio Control Module
Convergence Module
HVAC Module



Engine Control Module

Antilock Braking System Module

Power Steering Control Module

Headlamps Control Module

CAN C

Body Computer Module

OBD-II Port

CAN B

Parking Sensors Module

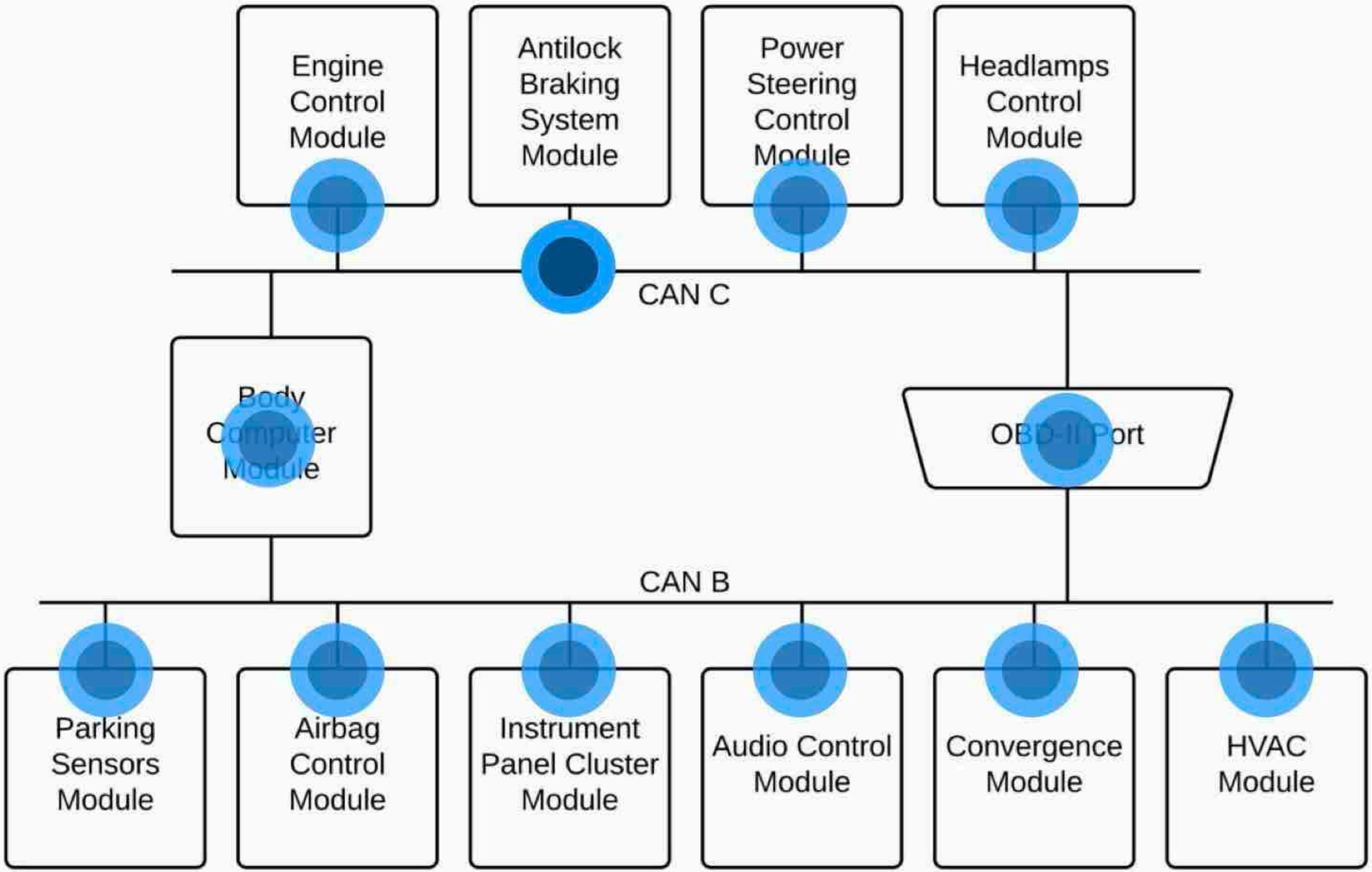
Airbag Control Module

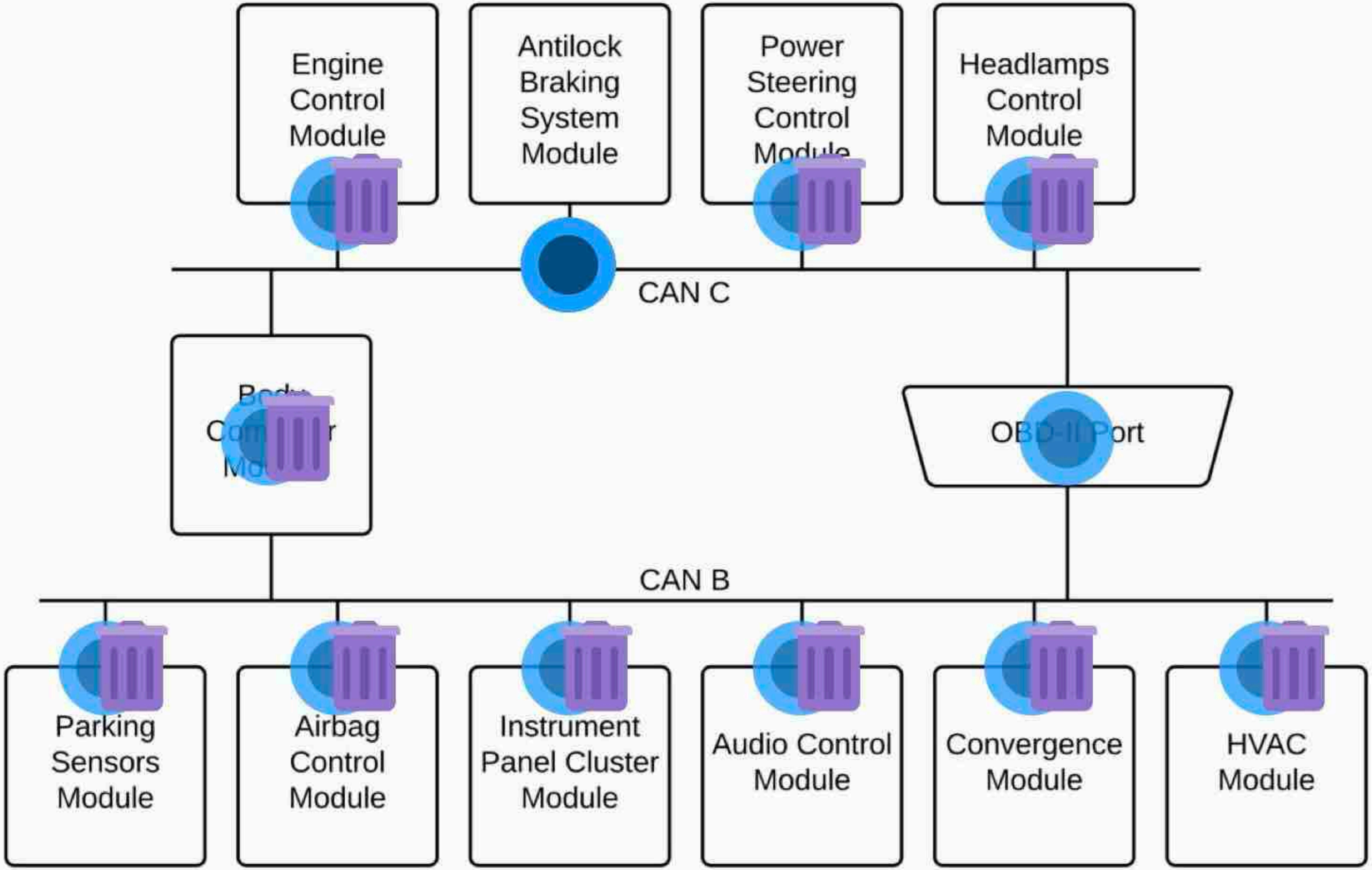
Instrument Panel Cluster Module

Audio Control Module

Convergence Module

HVAC Module


Engine Control Module
Antilock Braking System Module
Power Steering Control Module
Headlamps Control Module
CAN C
Body Computer Module
OBD-II Port
CAN B
Parking Sensors Module
Airbag Control Module
Instrument Panel Cluster Module
Audio Control Module
Convergence Module
HVAC Module



Engine Control Module

Antilock Braking System Module

Power Steering Control Module

Headlamps Control Module

CAN C

Body Computer Module

OBD-II Port

CAN B

Parking Sensors Module

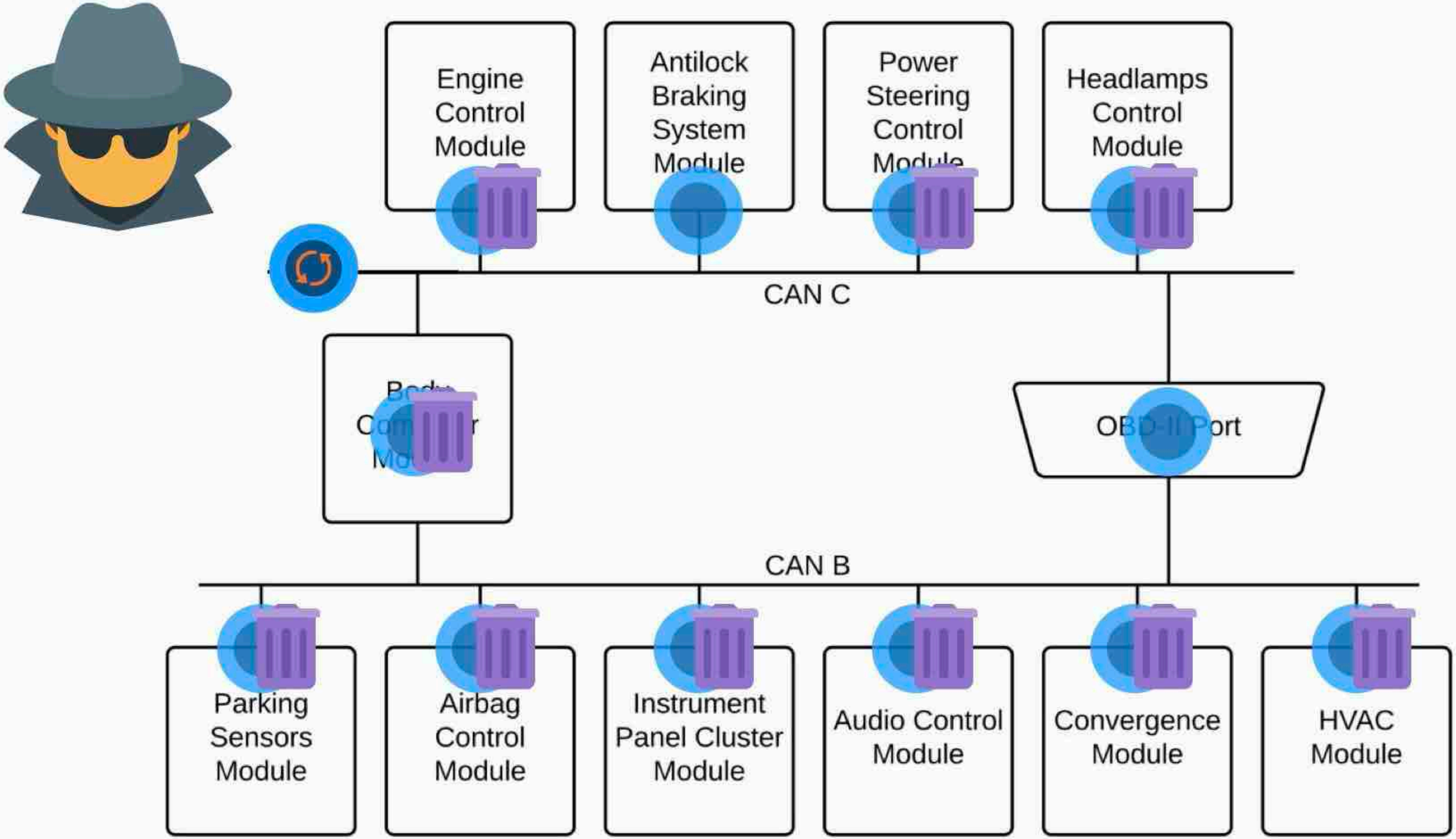
Airbag Control Module

Instrument Panel Cluster Module

Audio Control Module

Convergence Module

HVAC Module



Engine Control Module

Antilock Braking System Module

Power Steering Control Module

Headlamps Control Module

CAN C

Body Controller Module

OBD-II Port

CAN B

Parking Sensors Module

Airbag Control Module

Instrument Panel Cluster Module

Audio Control Module

Convergence Module

HVAC Module

No authentication

No authentication

No segmentation

Broadcast network

#1

No internal defences

#2

FACTORIES

14y

#2

Most attacked vertical

** IBM X-Force Research, 2016 Cyber Security Intelligence Index*

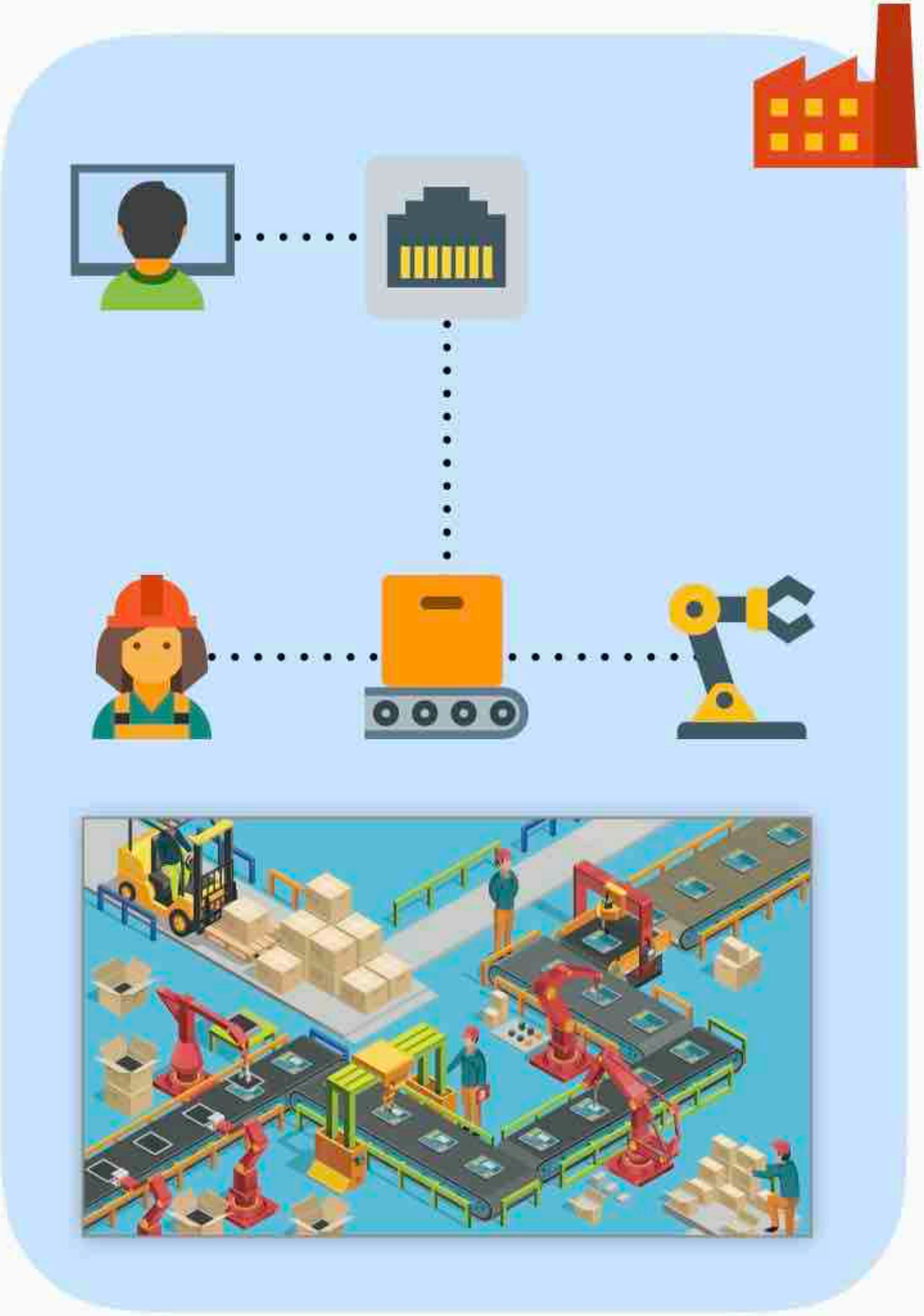
94%

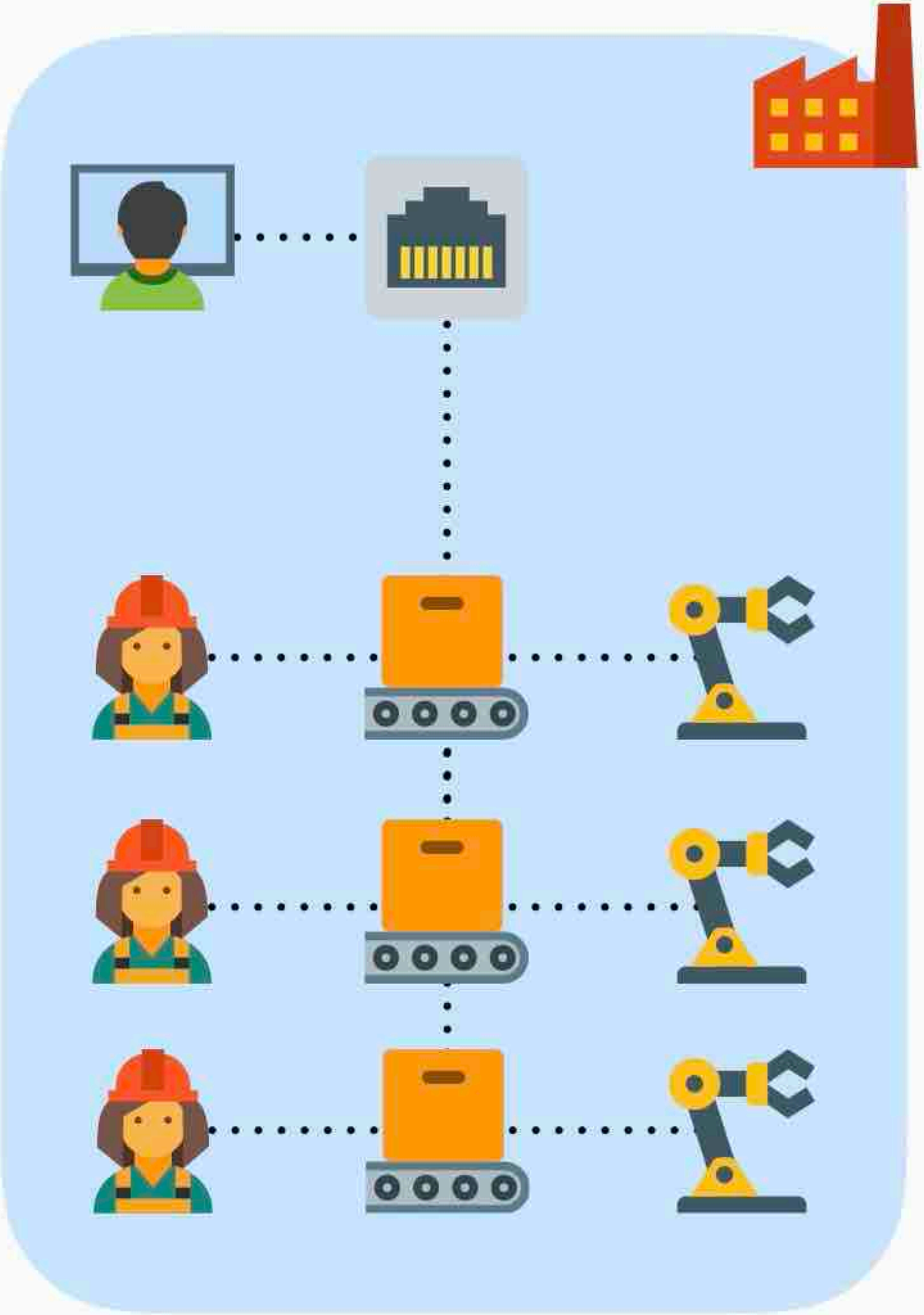
Attacks are espionage

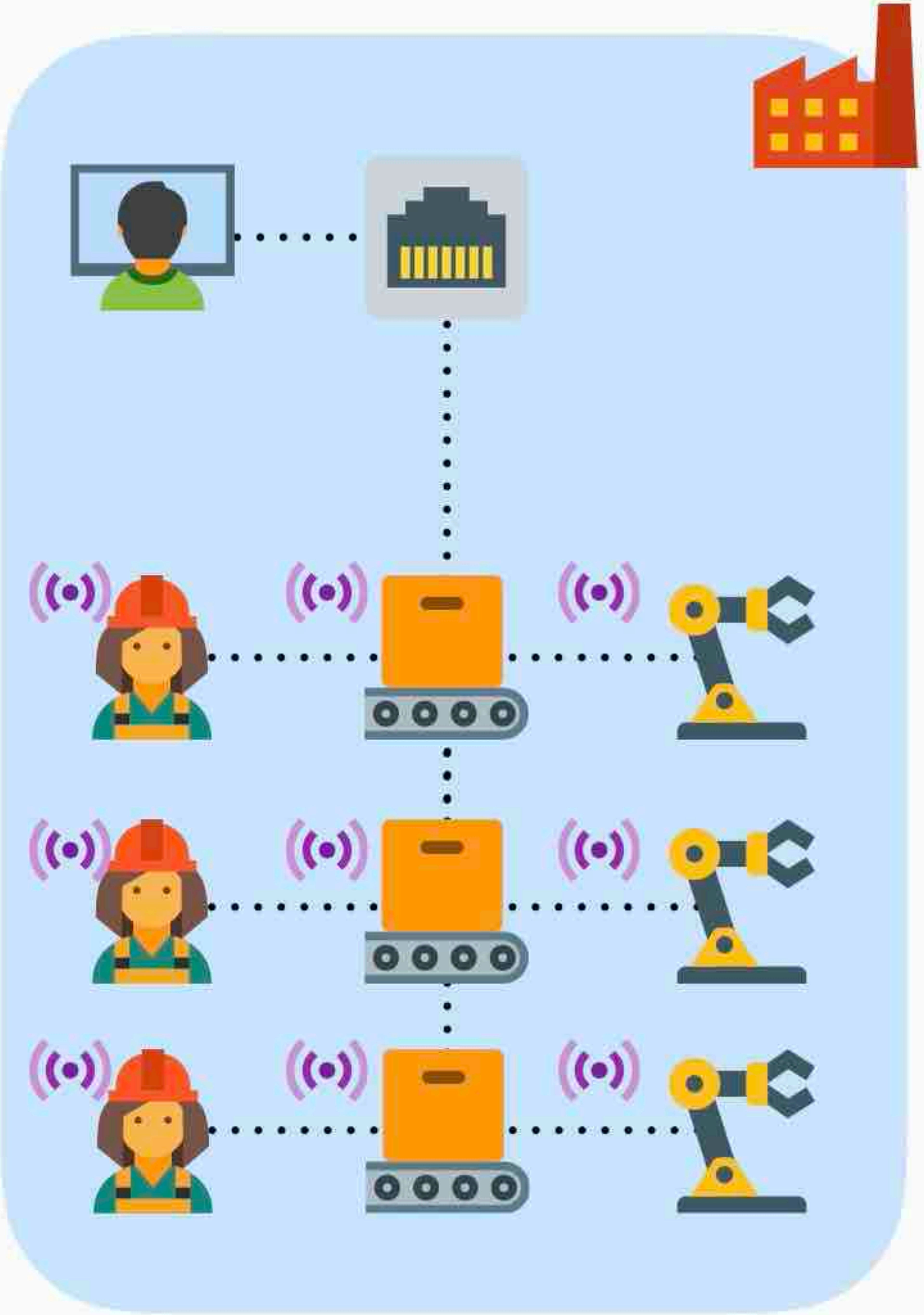
* *Verizon Data Breach Investigation Report, 2017*

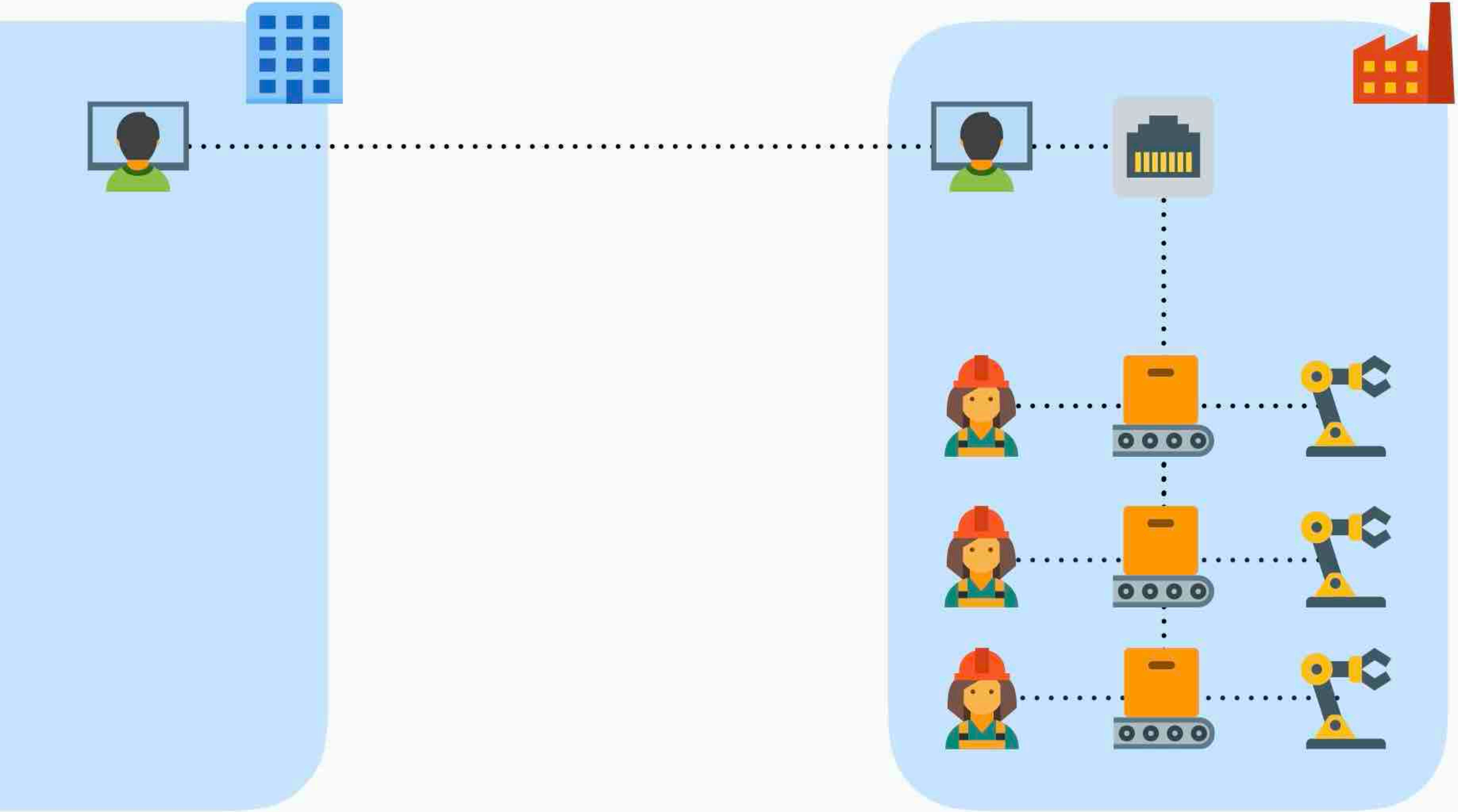
17%

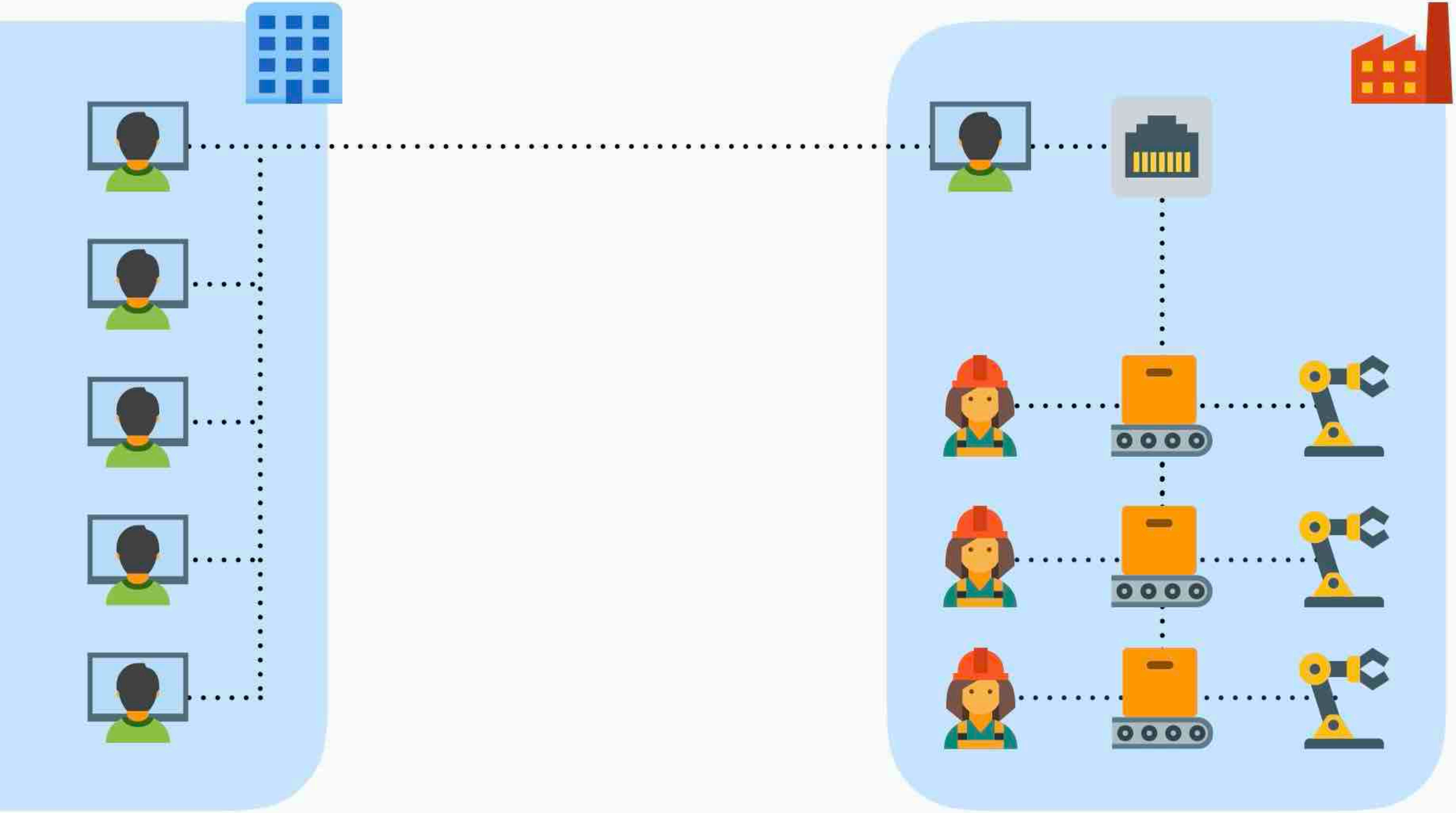
U.S. GDP

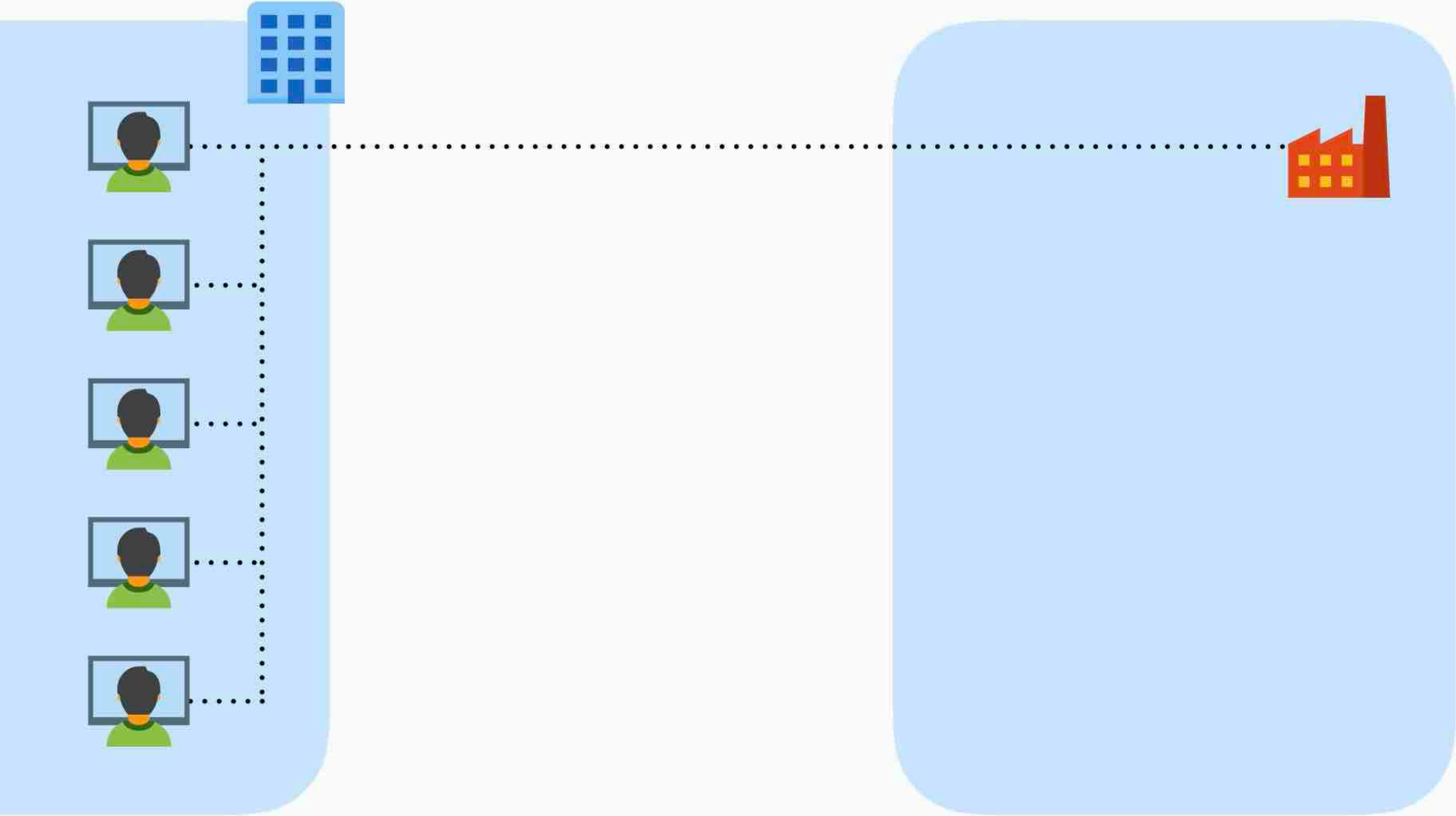


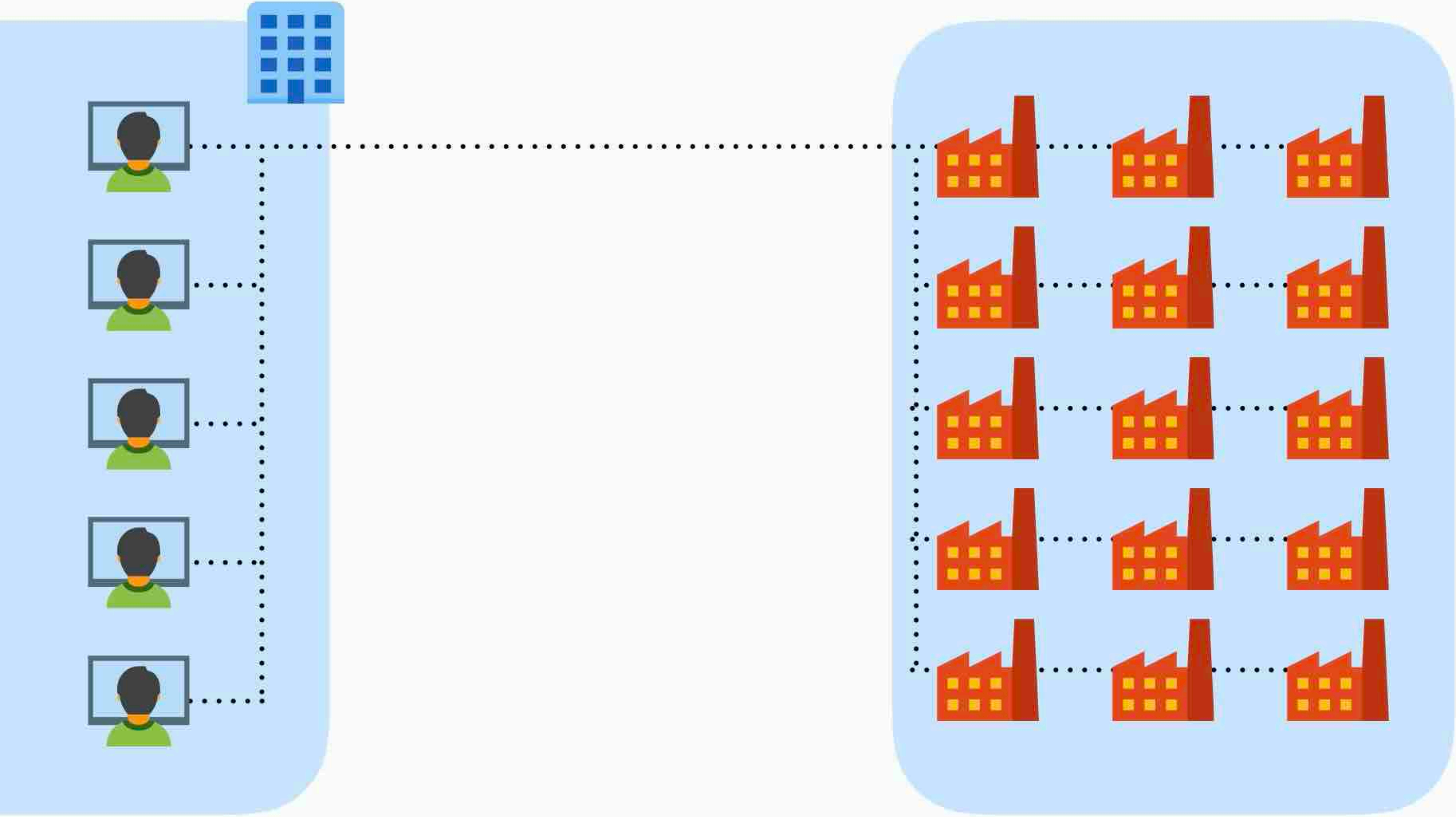








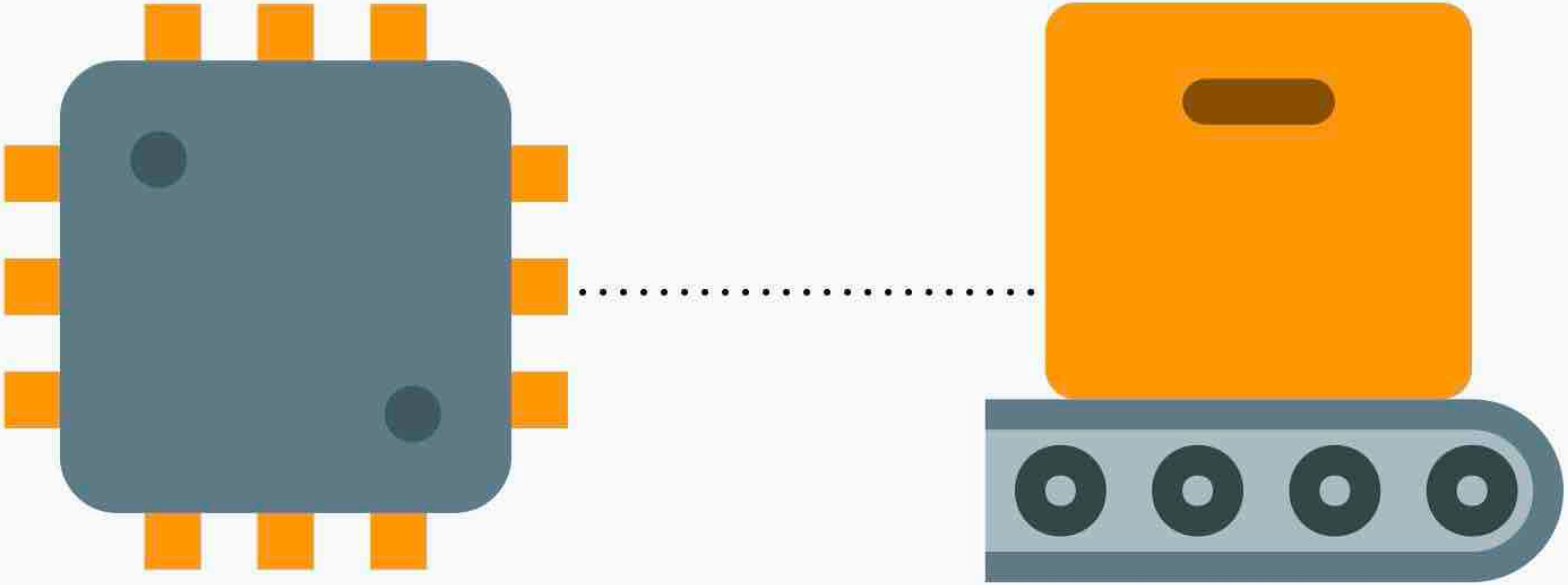




13%

success rate for phishing

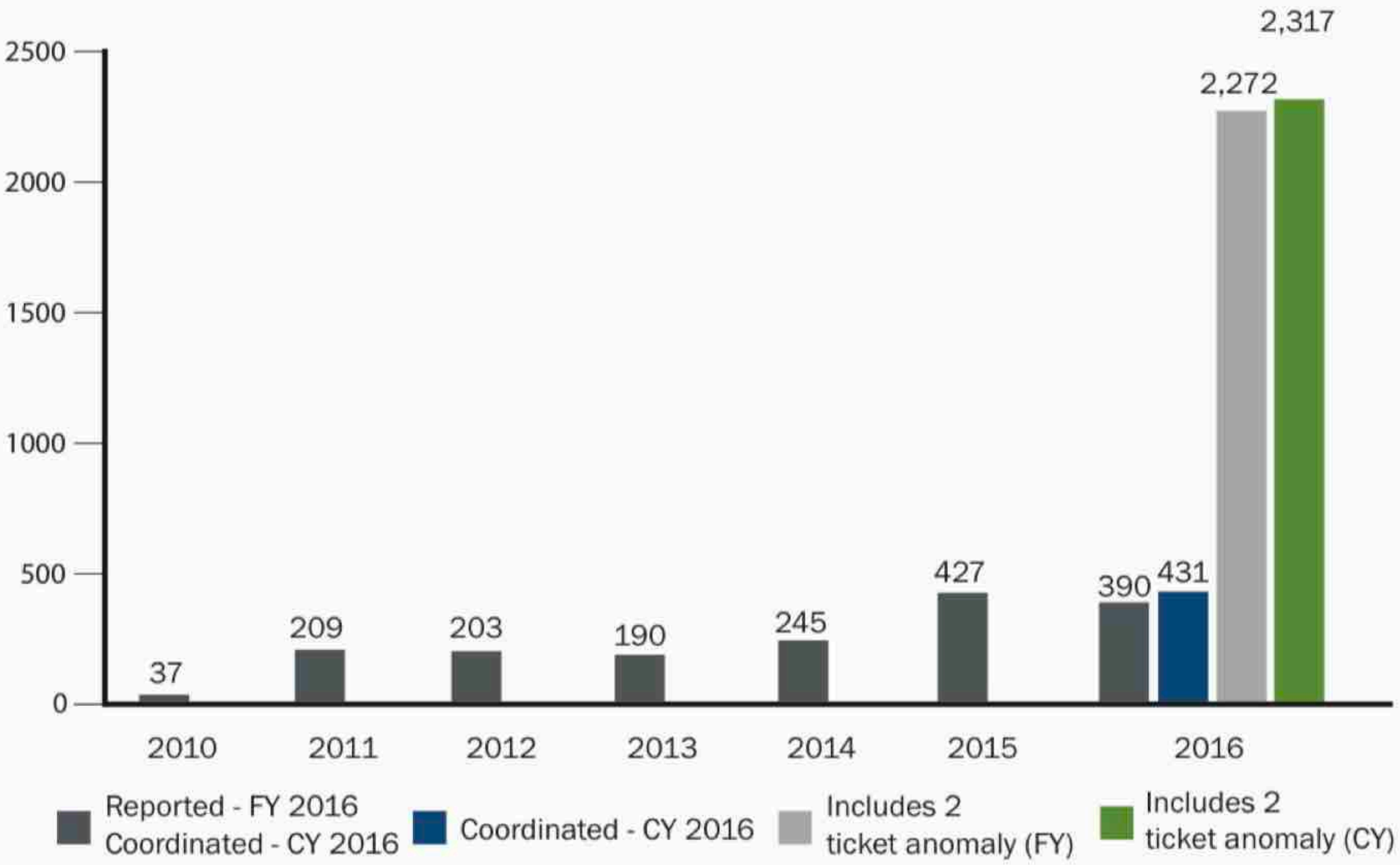
** Verizon Data Breach Investigation Report, 2017*



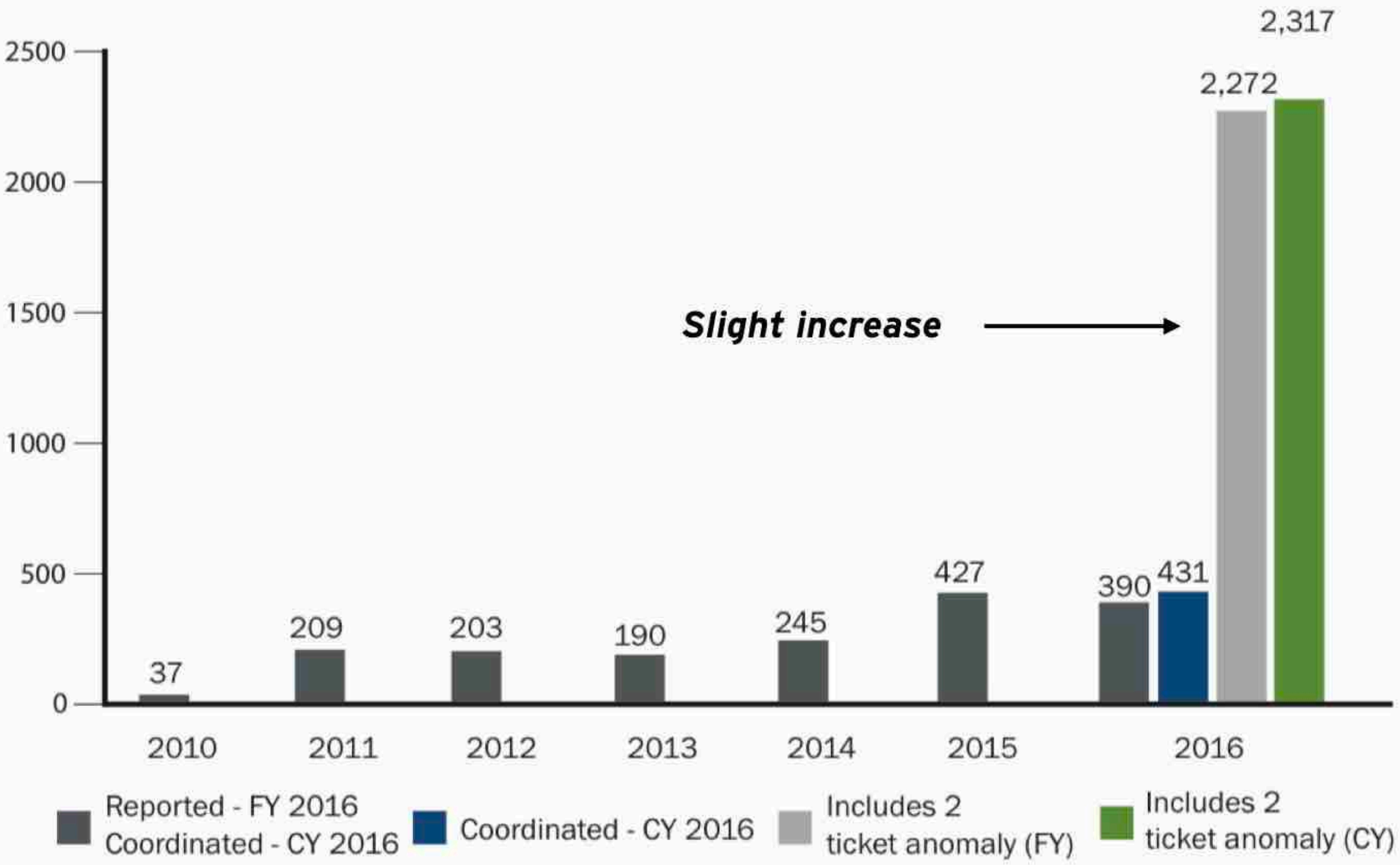
SCADA / ICS

Supervisory Control And Data Acquisition / Industrial Control Systems

S1
S2
M
alarm
on off
hard copy
key
7
8
9
clear
4
5
6
+
1
2
3
−
0
,
enter
F1
F2
F3
F4
F5
F6
B - 5001
B - 5003
B - 5002



** ICS-CERT reported & co-ordinated vulnerability disclosures*



Slight increase

** ICS-CERT reported & co-ordinated vulnerability disclosures*

Hostile networks

#3

Vulnerable devices

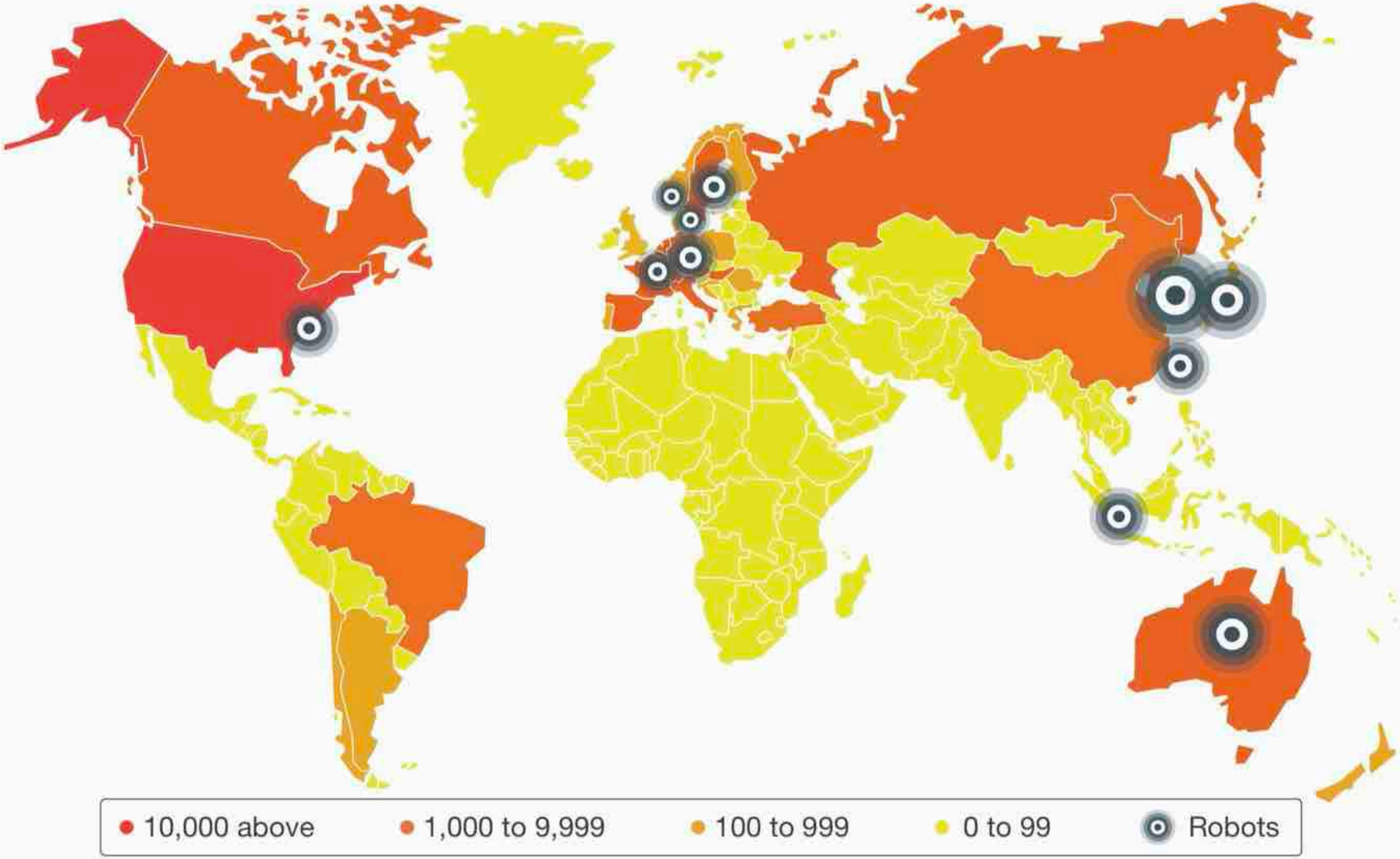
#4

ARMS

8y

6lbs max
19" reach

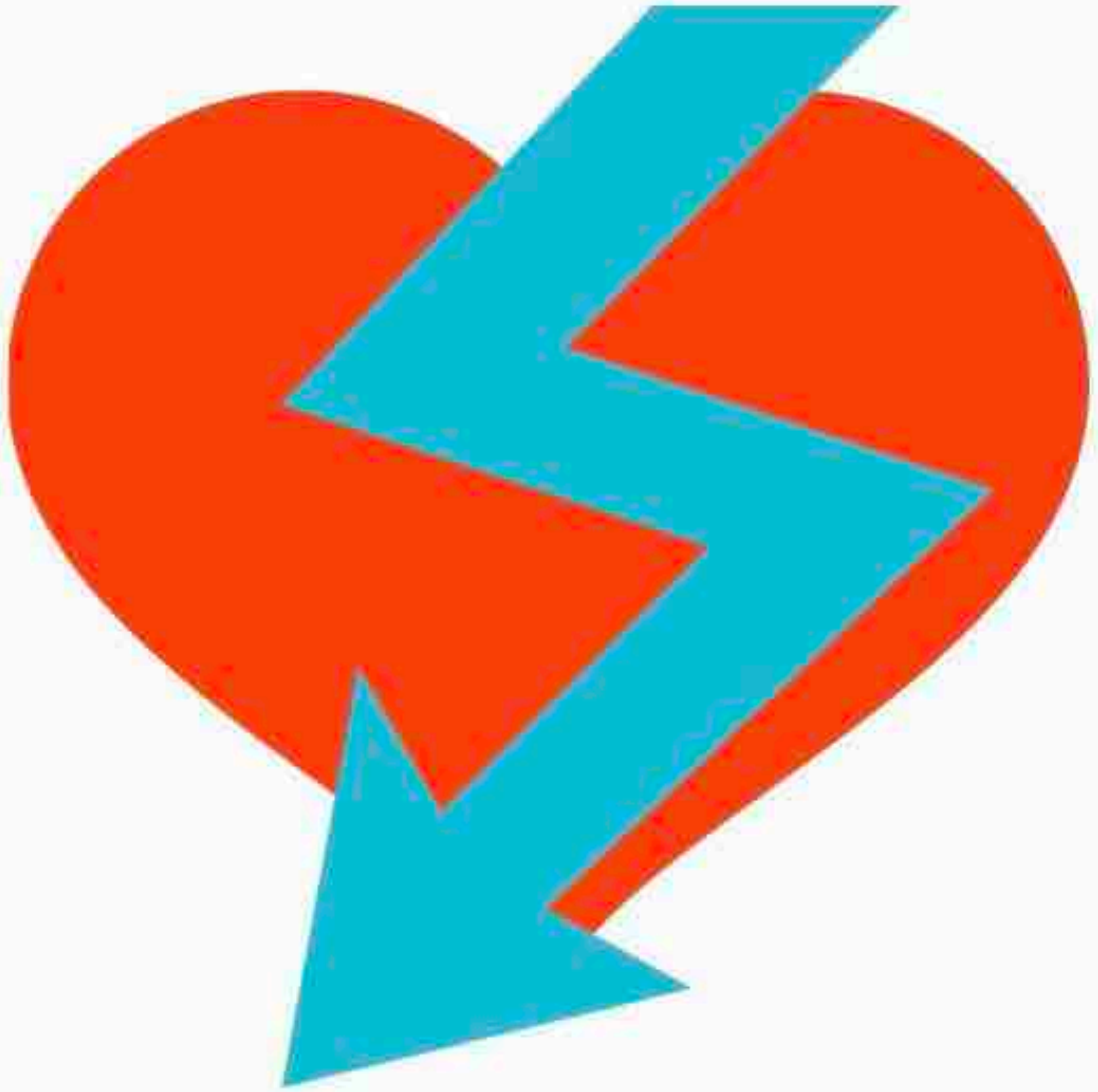
1700lbs max
13'9" reach



** Volume of exposed industrial routers and presence of exposed robots*

Cyber-physical System

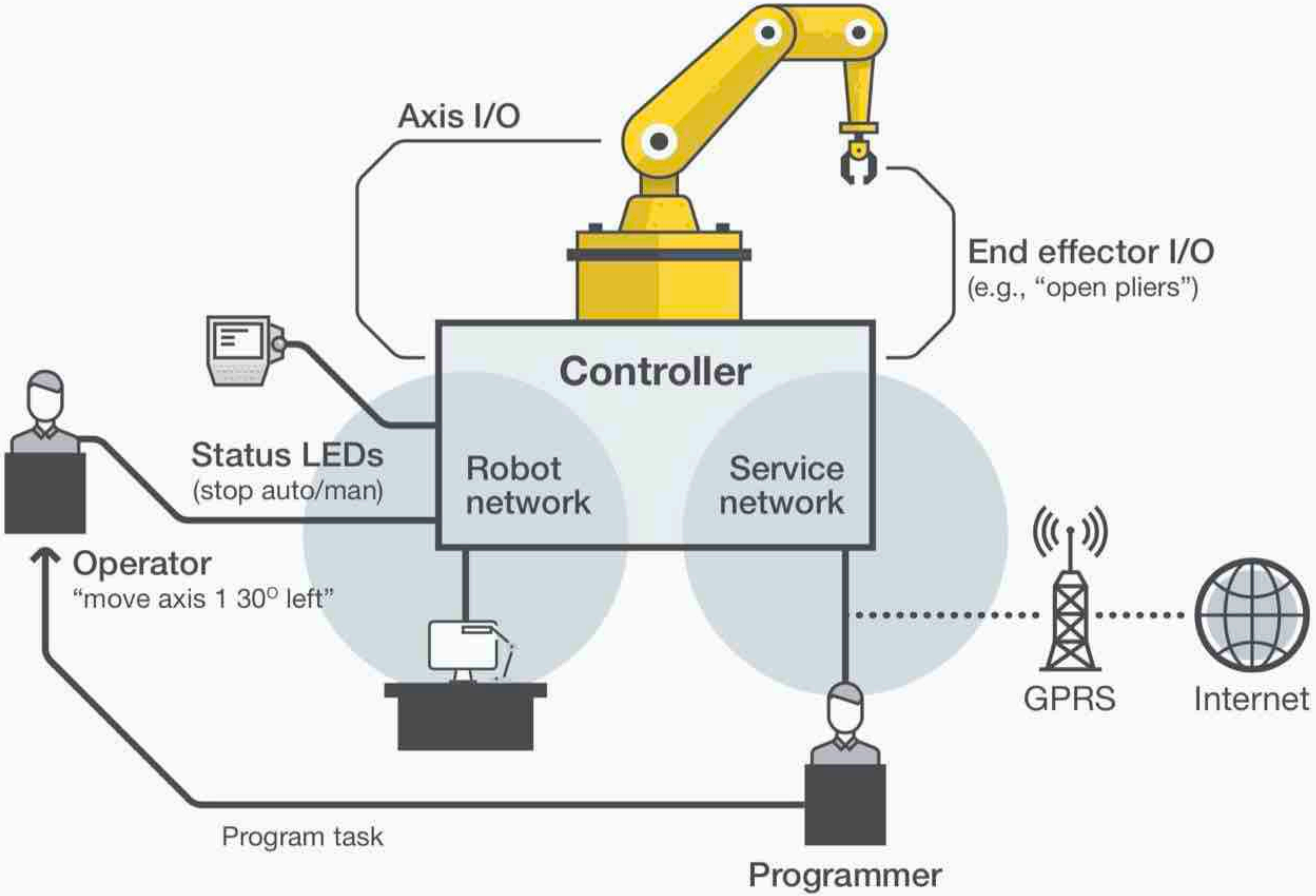
Robot + human



Zero risk tolerance

Safety regulations

** Does not include cyber*



Standard architecture for articulated robotic arms

Some problems...

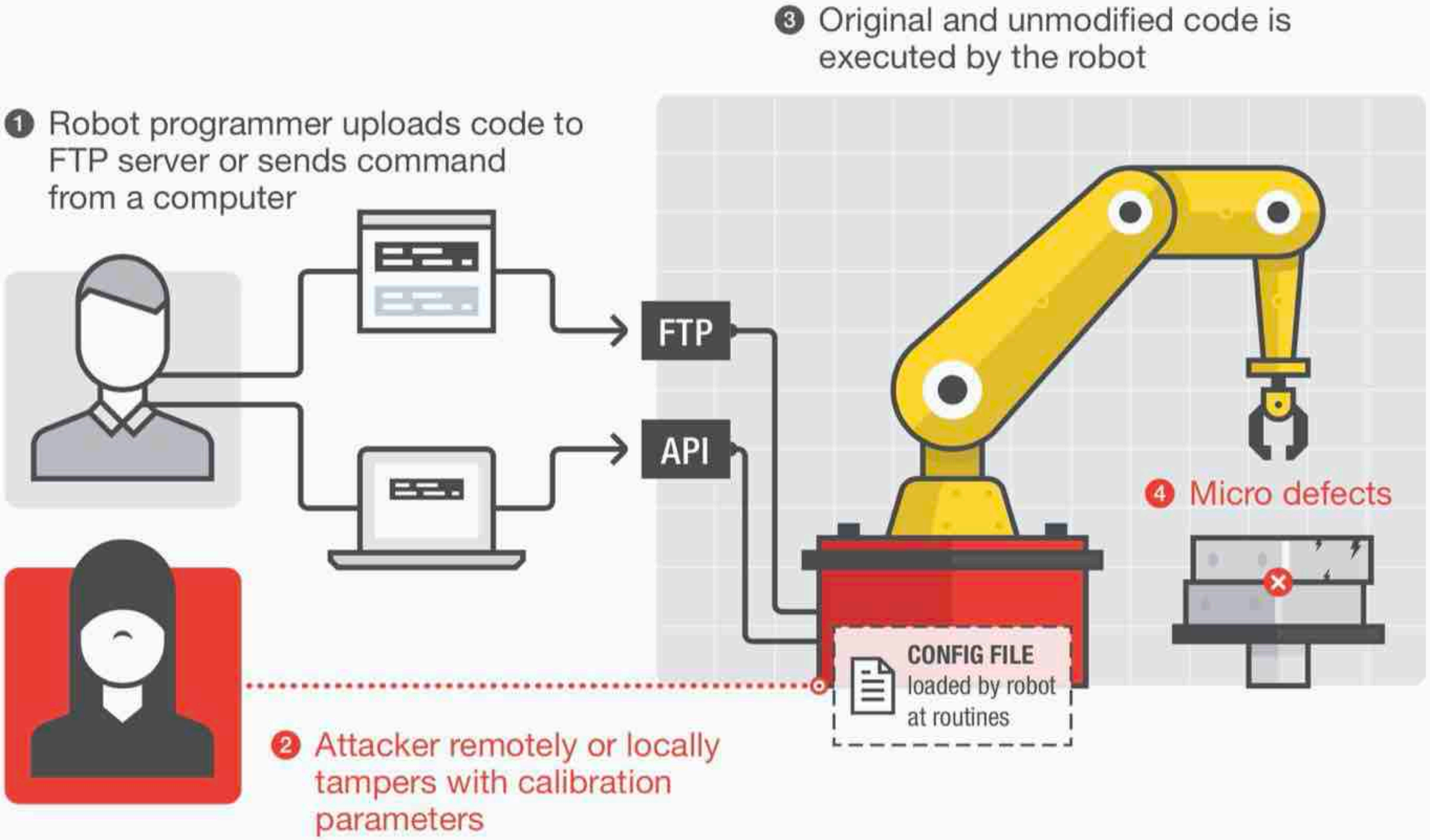
Poor encryption

Outdated software

Poor/no authentication

Insecure interfaces

No code signing



❸ Original and unmodified code is executed by the robot
❶ Robot programmer uploads code to FTP server or sends command from a computer
FTP
API
❹ Micro defects
CONFIG FILE
loaded by robot
at routines
❷ Attacker remotely or locally tampers with calibration parameters

Adjust configuration to produce defects in product

First we sh strial
robot that w ammed to
run a simple task: “draw a
straight line.”

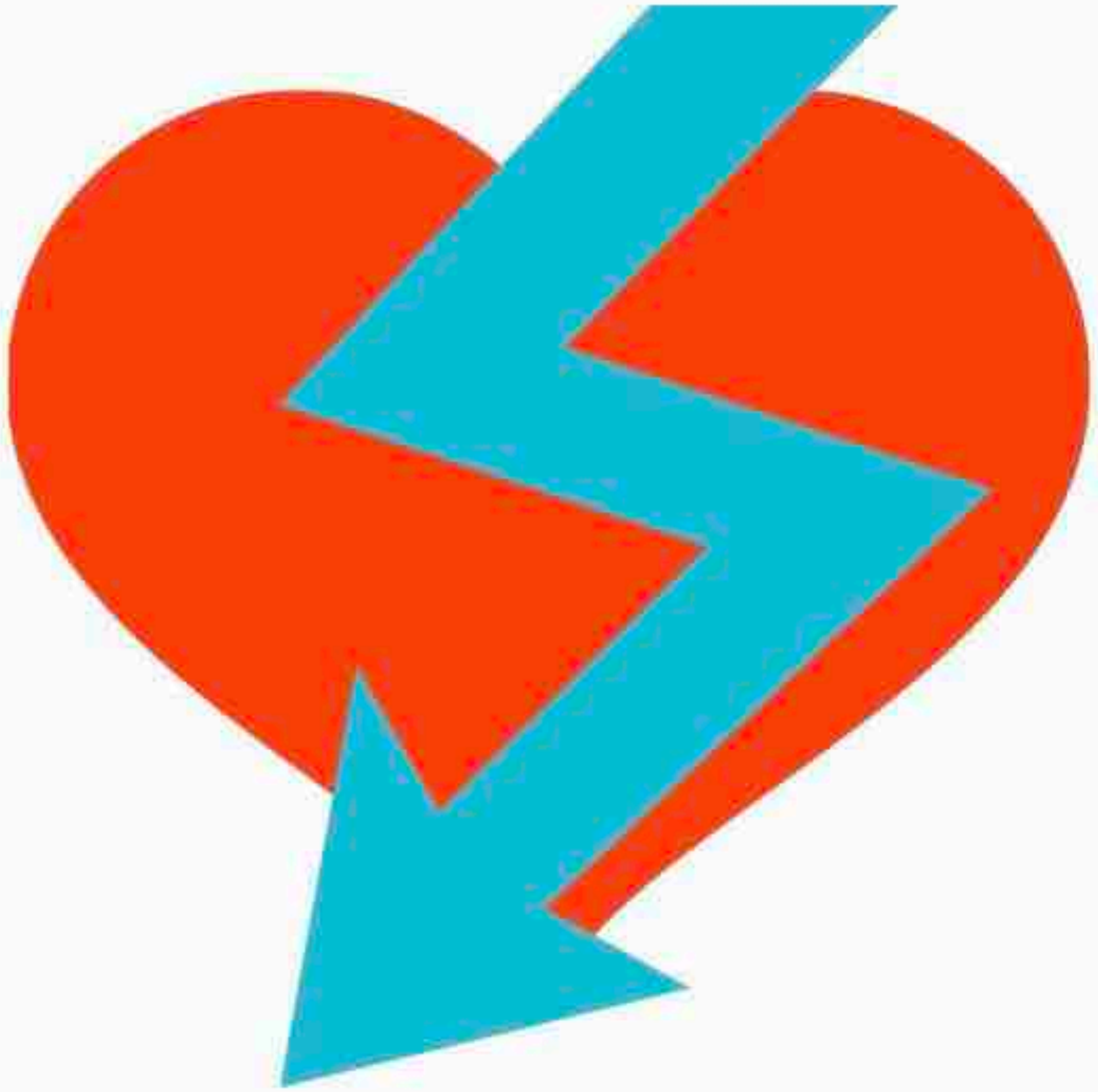
Known vulnerabilities

#5

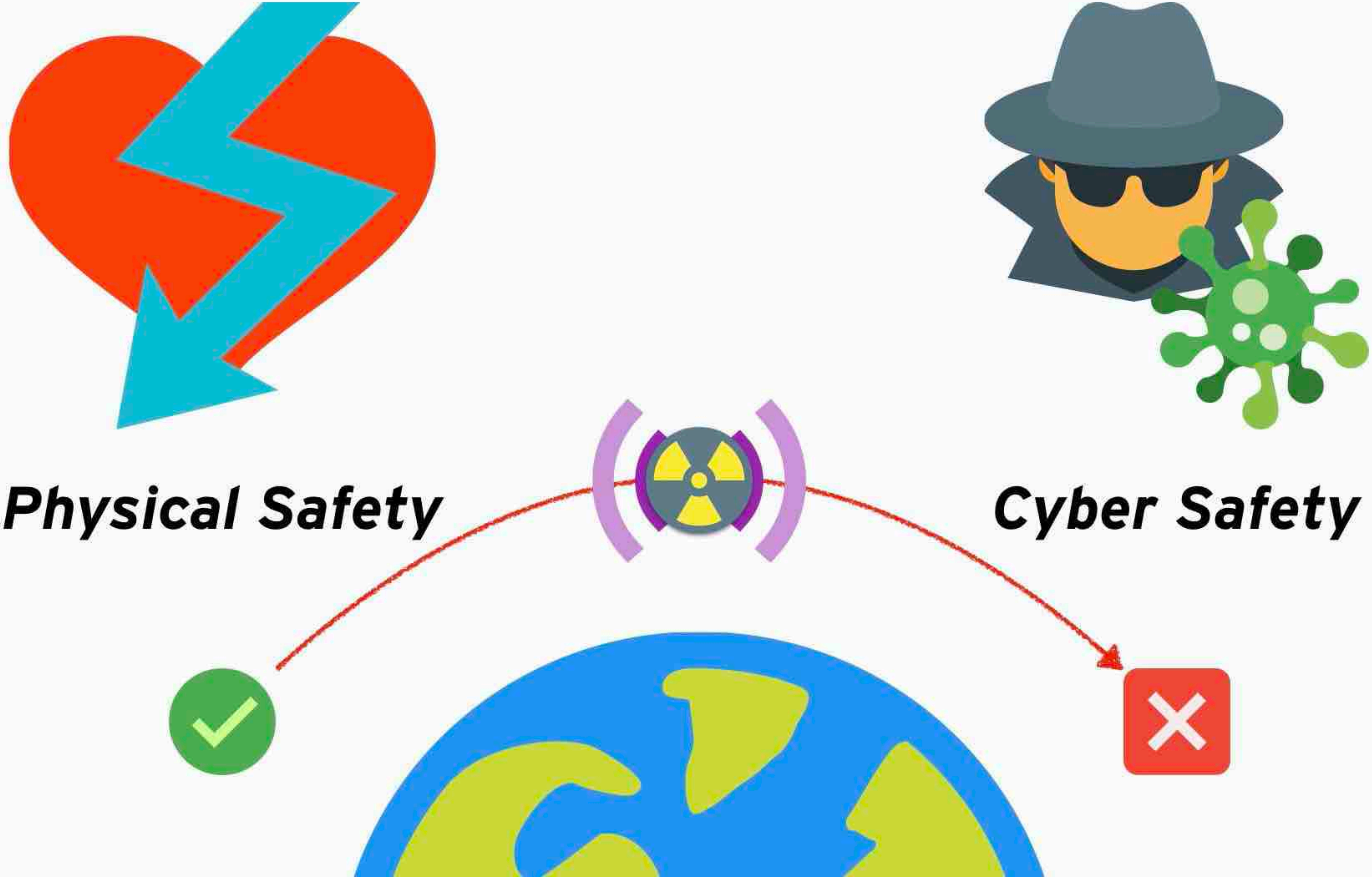
Exposed deployments

#6

WHERE TO?



Physical Safety



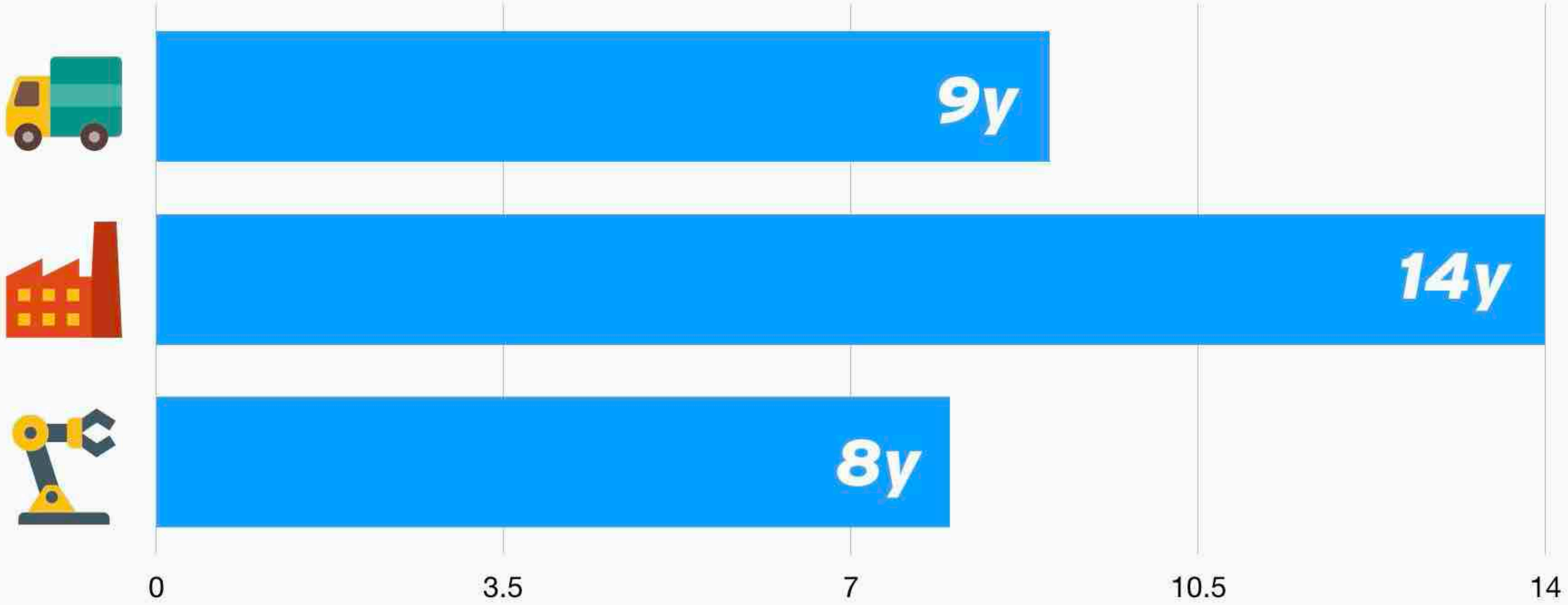
Physical Safety

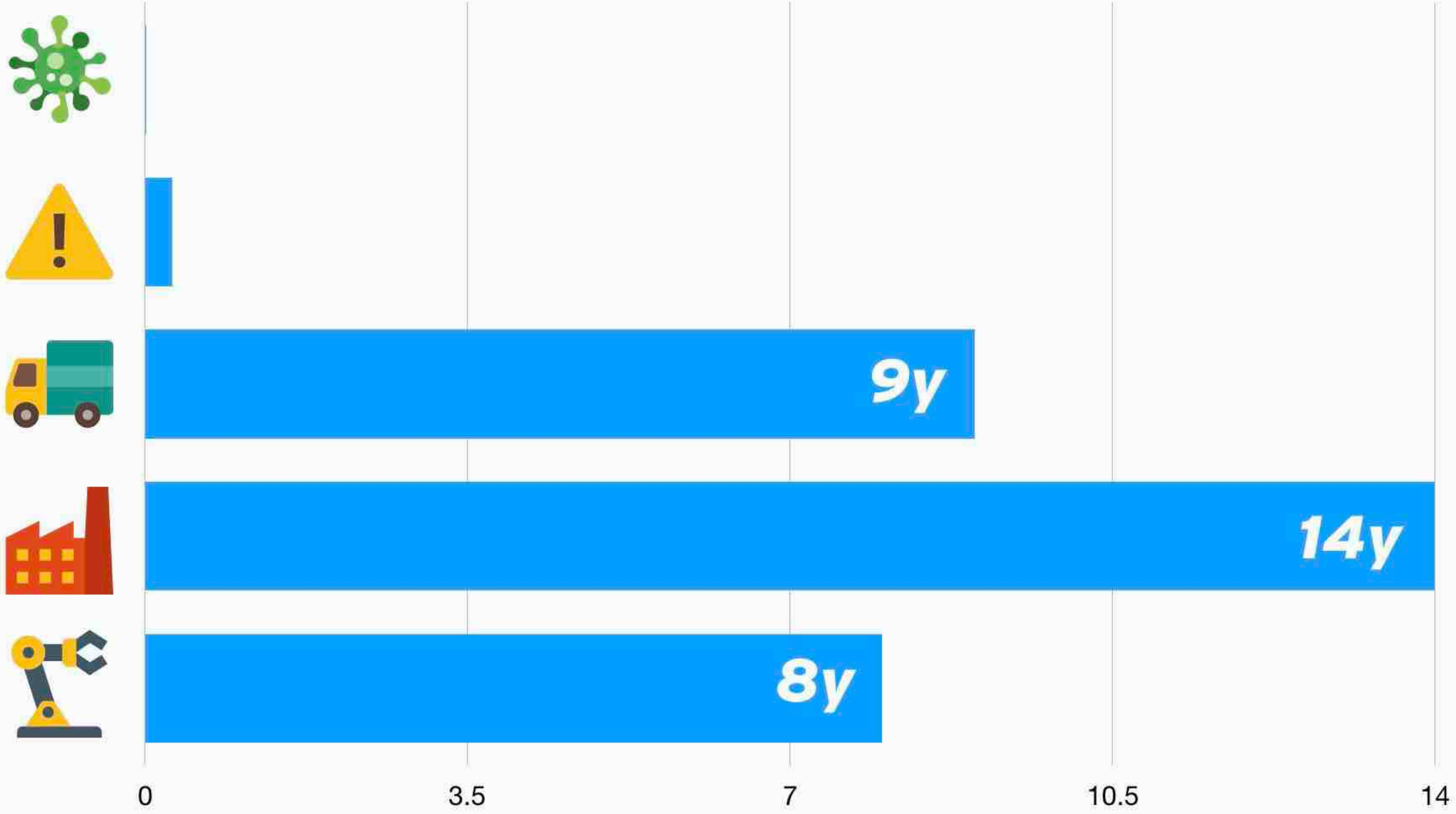
Cyber Safety

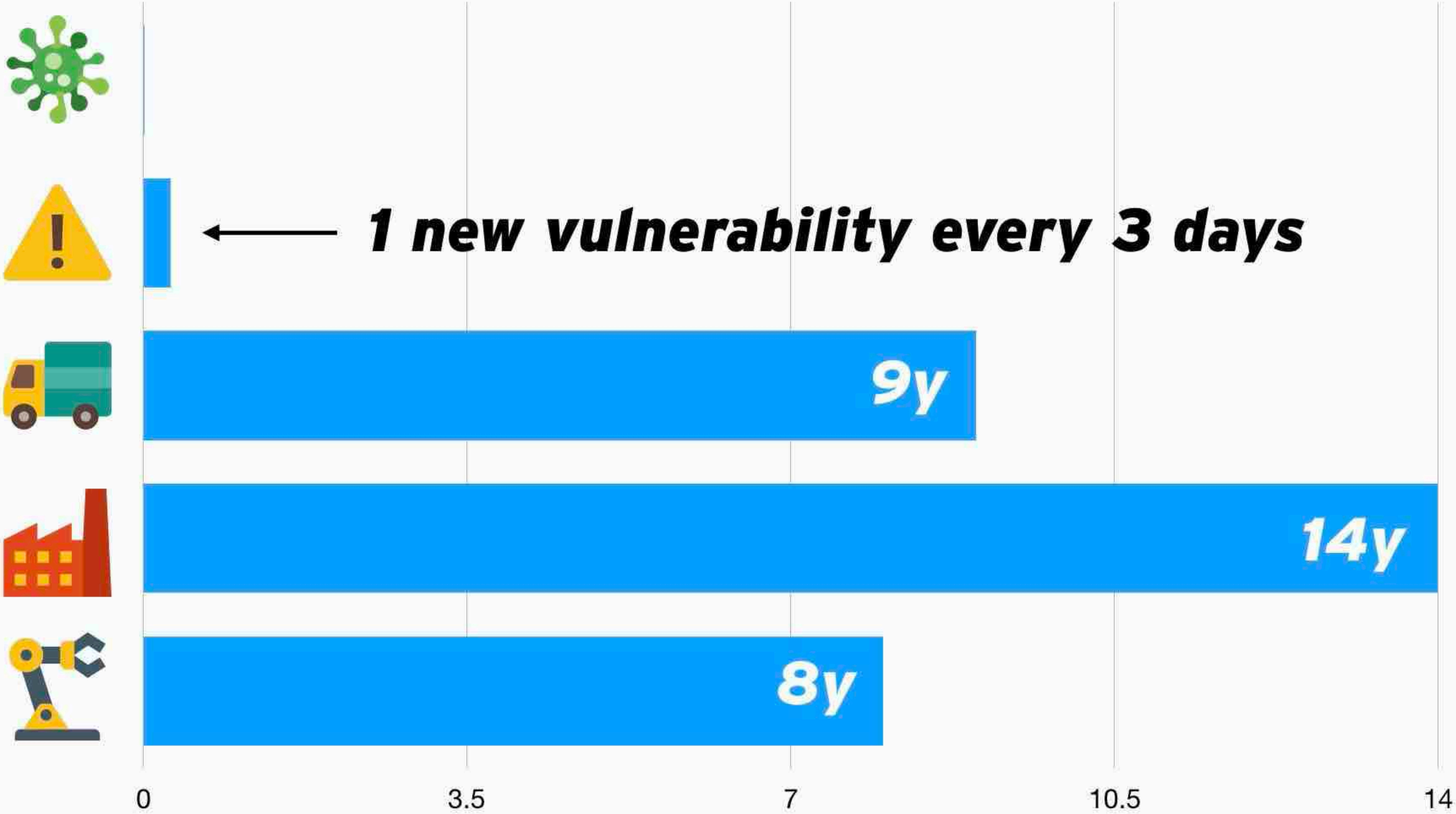
Broadcast networks
No internal defences

Hostile networks
Vulnerable devices

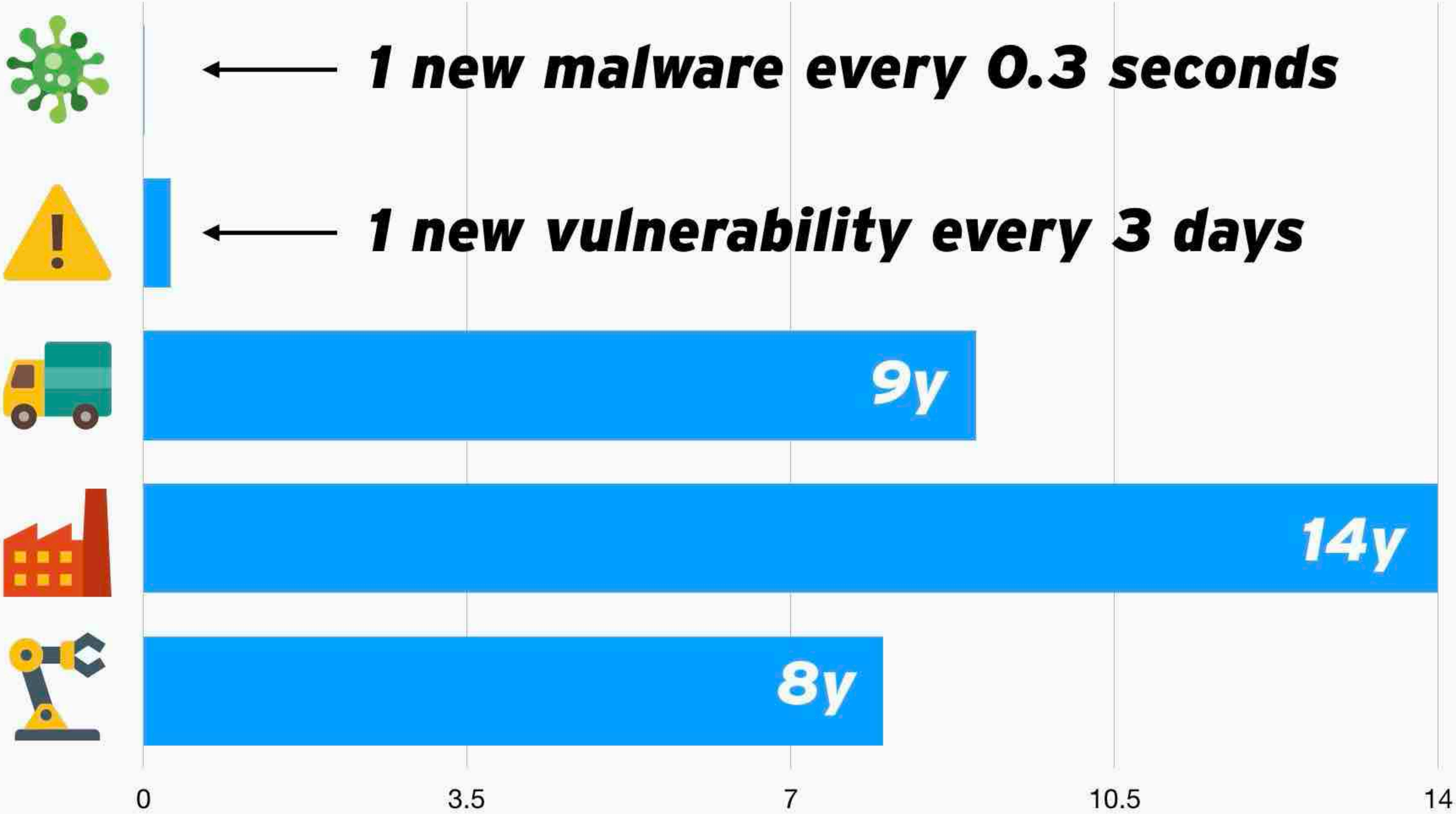
Known vulnerabilities
Exposed devices


9y
14y
8y
0
3.5
7
10.5
14


9y
14y
8y
0
3.5
7
10.5
14



1 new vulnerability every 3 days



1 new malware every 0.3 seconds

1 new vulnerability every 3 days

The goal of cybersecurity

Make sure that systems work as intended ...and ONLY as intended

Thank you!

4mn.ca/sxsw18-rogue-robots

Mark Nunnikhoven

Vice President, Cloud Research, Trend Micro

@marknca

A special thanks to the efforts of the combined team from Trend Micro Research and the Politecnico di Milano for the technical analysis of the state of articulated robotic arms and the CAN bus standard

TREND MICRO™

POLITECNICO DI MILANO