セッションID：E-1

IT Risks and Threats on Safety of Operational Technology

A Case Study on Wireless Remote Controllers from the Eyes of the Attackers

トレンドマイクロ株式会社
Trend Micro Research

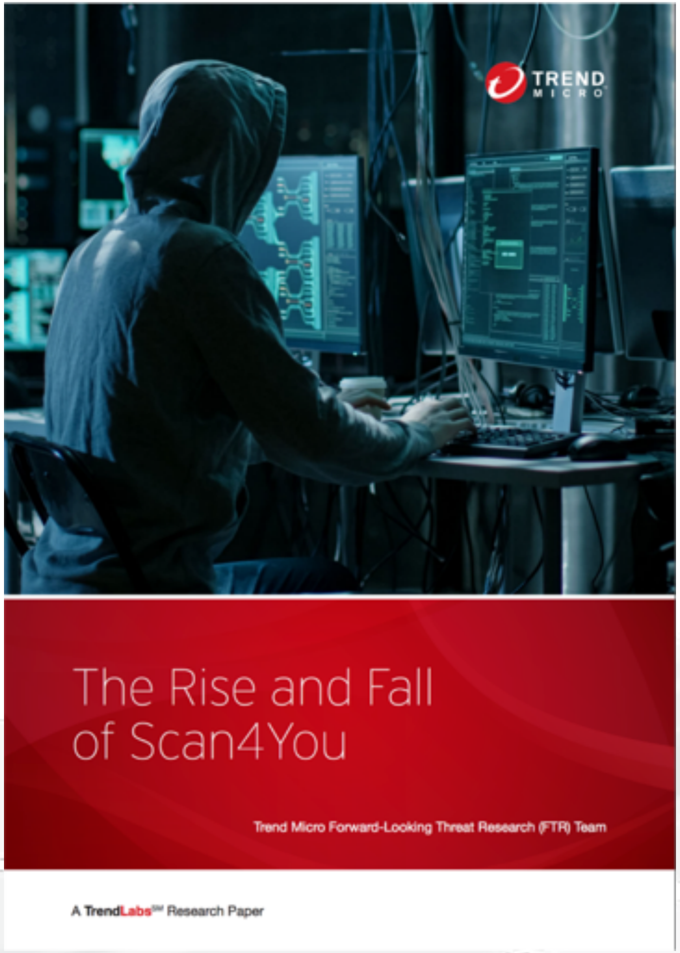
Federico Maggi, PhD / @phretor
Senior Threat Researcher

TREND MICRO | research

CYBERCRIME TECHNOLOGY SOCIAL

CYBERCRIME RESEARCH

"Tracking & predicting the cybercrime underground"



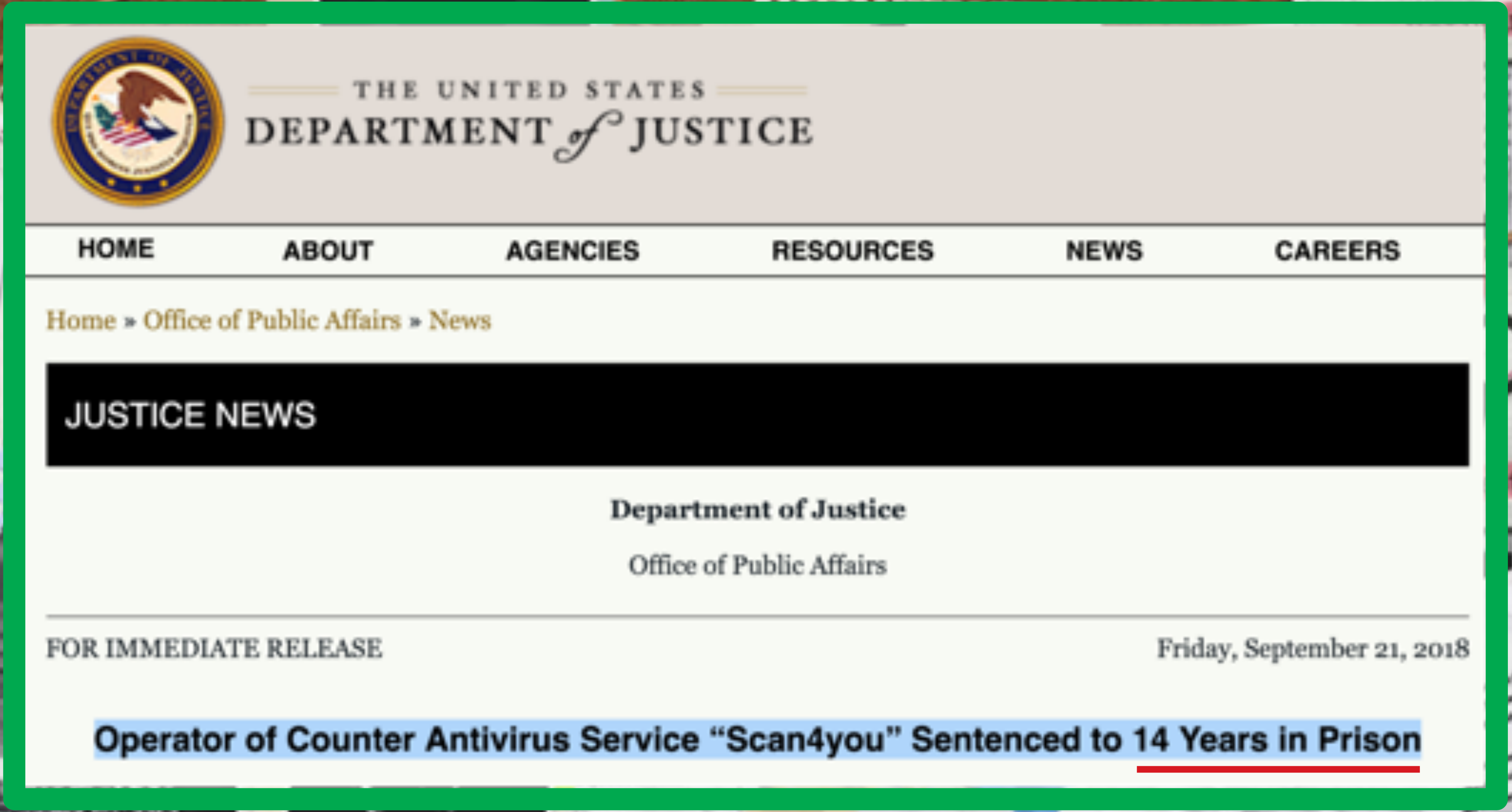
The Rise and Fall of Scan4You

Trend Micro Forward-Looking Threat Research (FTR) Team

A TrendLabs℠ Research Paper

CYBERCRIME RESEARCH

"Taking down a **key service** critical to the **entire** cyber underground"



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, September 21, 2018

Operator of Counter Antivirus Service "Scan4you" Sentenced to 14 Years in Prison

TECHNOLOGY RESEARCH

“Risks and threats of a technology”

TREND MICRO

Rogue Robots: Testing the Limits of an Industrial Robot's Security

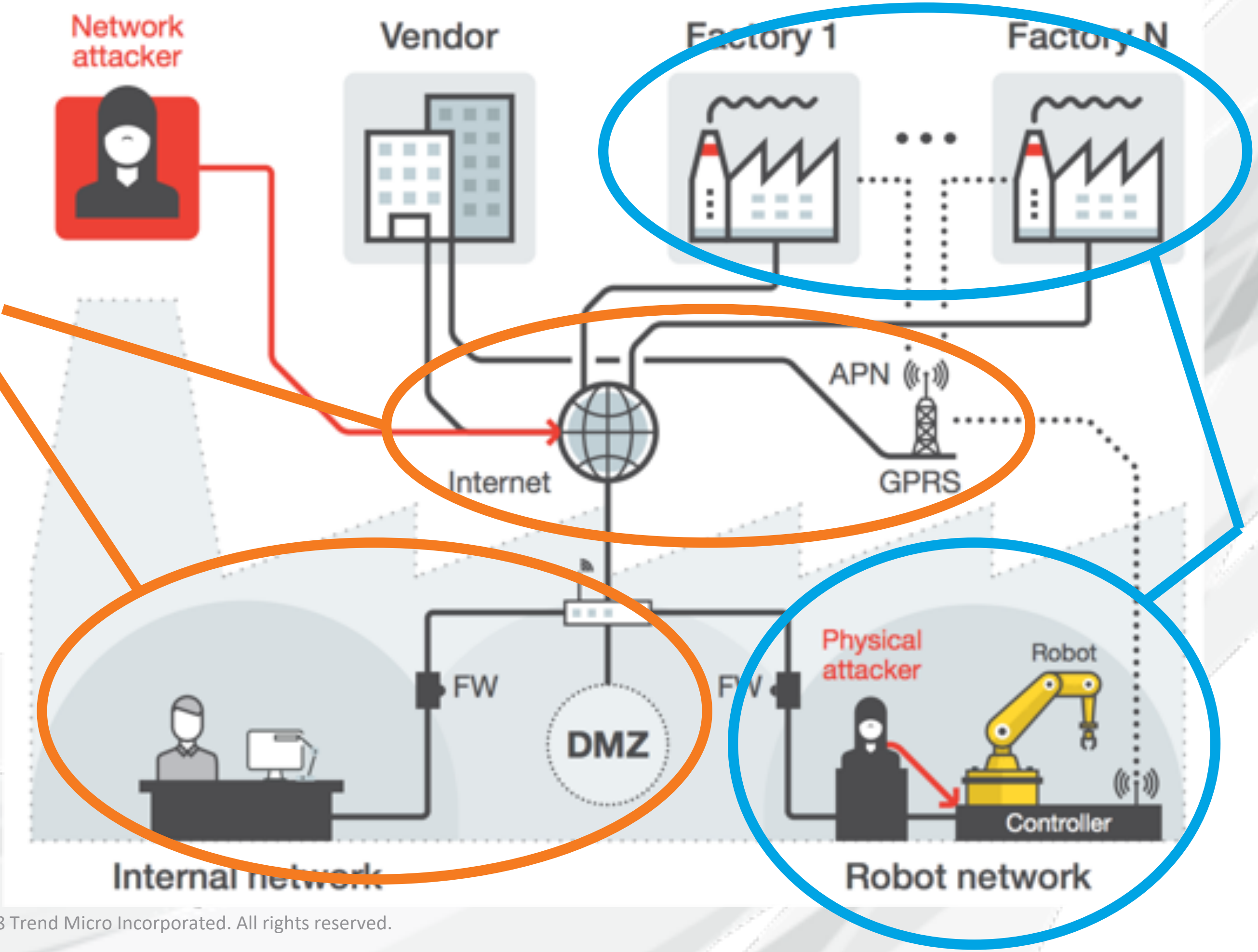
Federico Maggi
Trend Micro Forward-Looking Threat Research

Davide Quarta, Marcello Pogliani, Mario Polino,
Andrea M. Zanchettin, and Stefano Zanero
Politecnico di Milano

A TrendLabs Research Paper

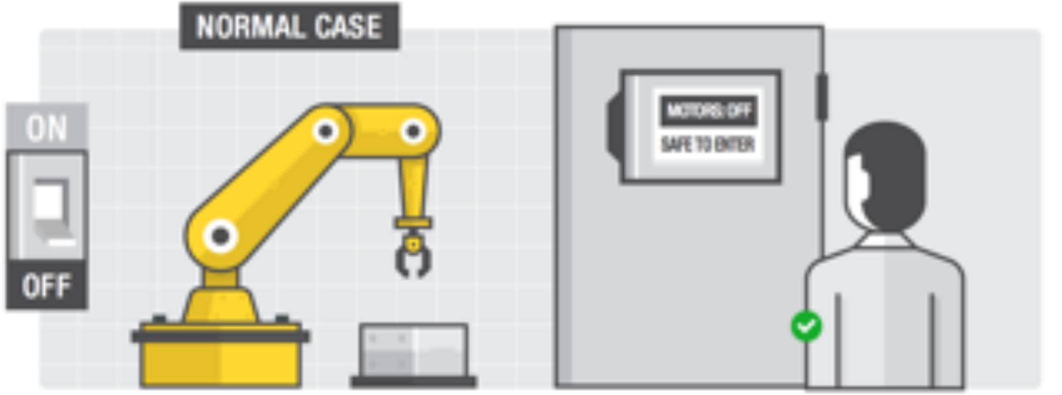
TECHNOLOGY RESEARCH

“Risks and threats of **upcoming** or **trendy** technology”

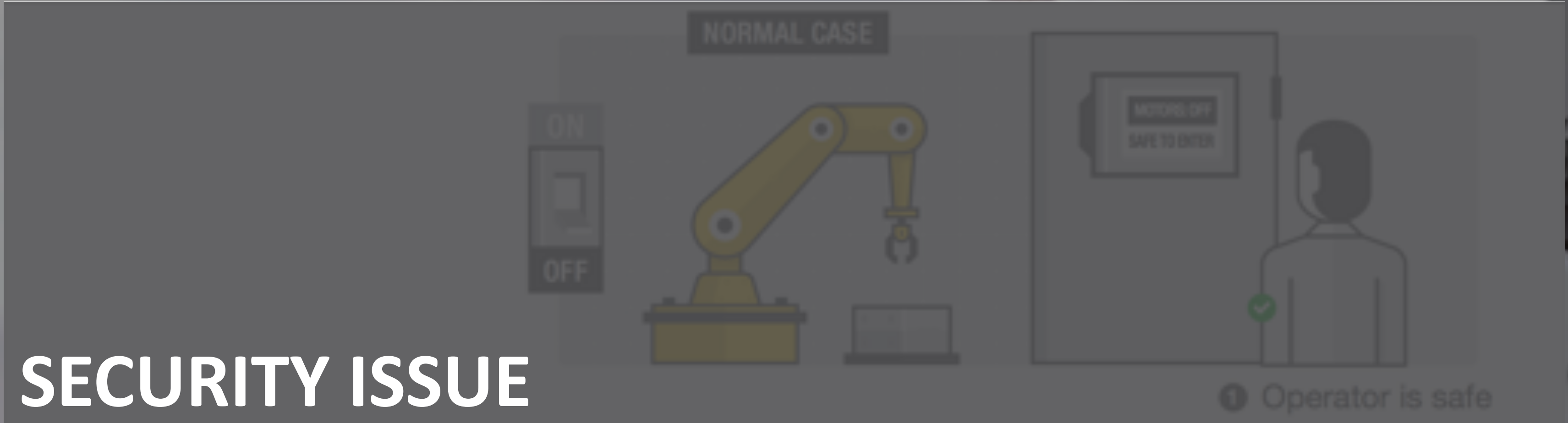


Information Technology (IT)

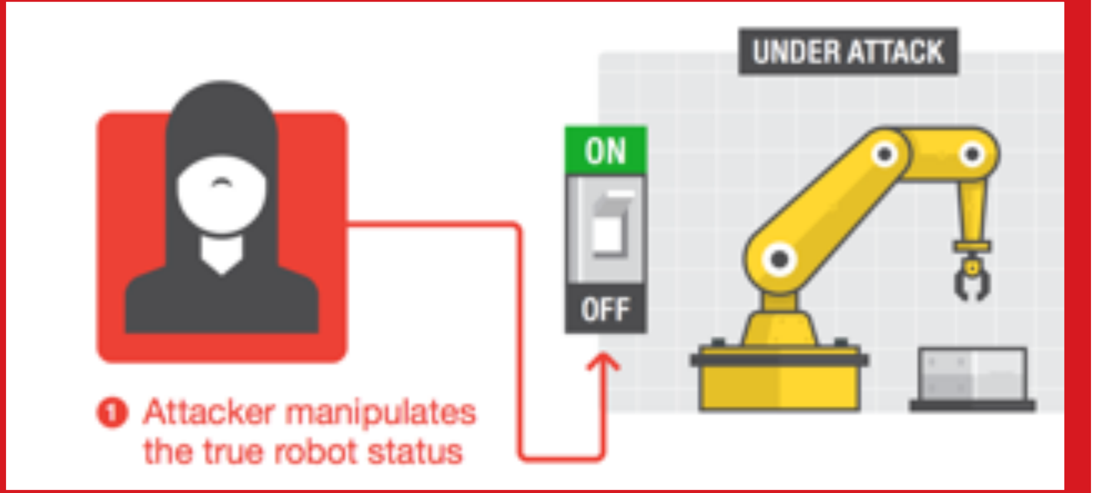
Operational Technology (OT)



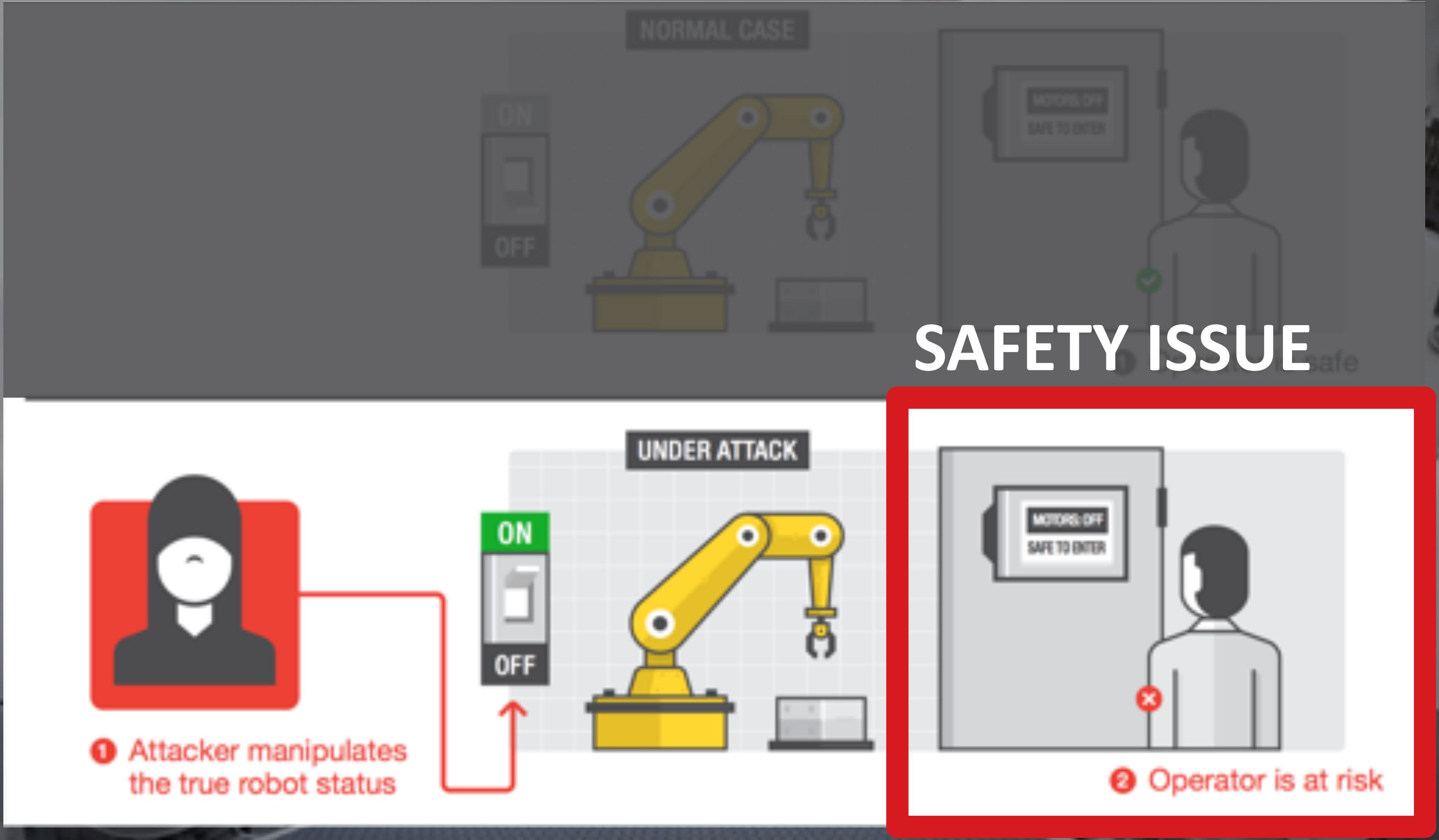
❶ Operator is safe



SECURITY ISSUE



SAFETY ISSUE



A Security Analysis of Radio Remote Controllers for Industrial Applications

Jonathan Andersson, Marco Balduzzi, Stephen Hilt, Philippe Lin, Federico Maggi, Akira Urano, and Rainer Vosseler

TECHNOLOGY RESEARCH

“Risks and threats of **widely used** technology”

Jonathan Anderson
Marco Balduzzi
Stephen Hilt
Philippe Lin
Federico Maggi
Akira Urano
Rainer Vosseler

Paper release: coming soon!

[redacted]

Where are they **used**?

How do they **work**?

What are the **risks**?

Where are they used?

How do they work?

What are the risks?

INDUSTRIAL HOISTS

MOBILE HOISTS

CONCRETE PUMPS

AGRICULTURE

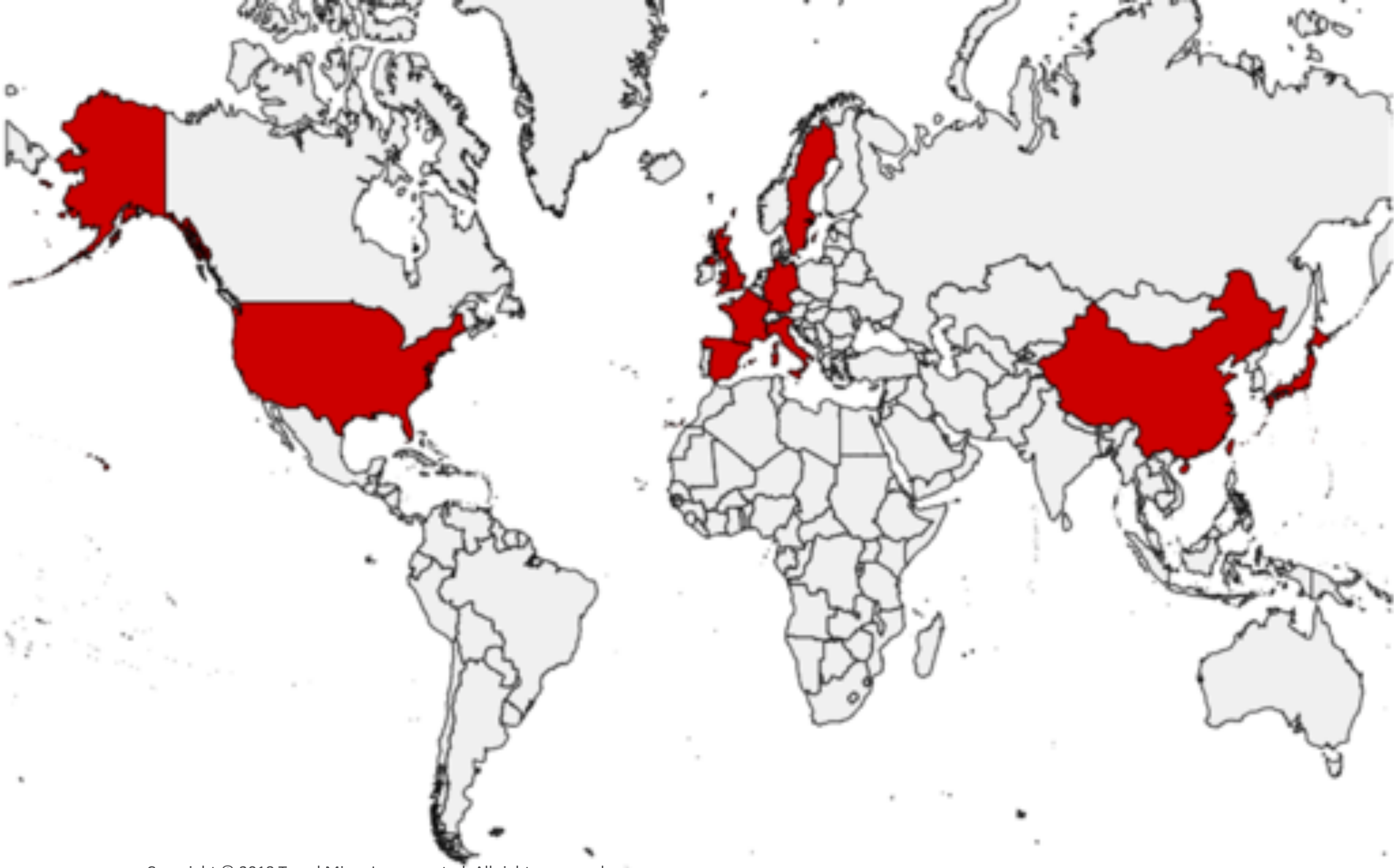
LOGISTICS

FORESTRY

DRILLING OPERATIONS

INDUSTRIAL AUTOMATION

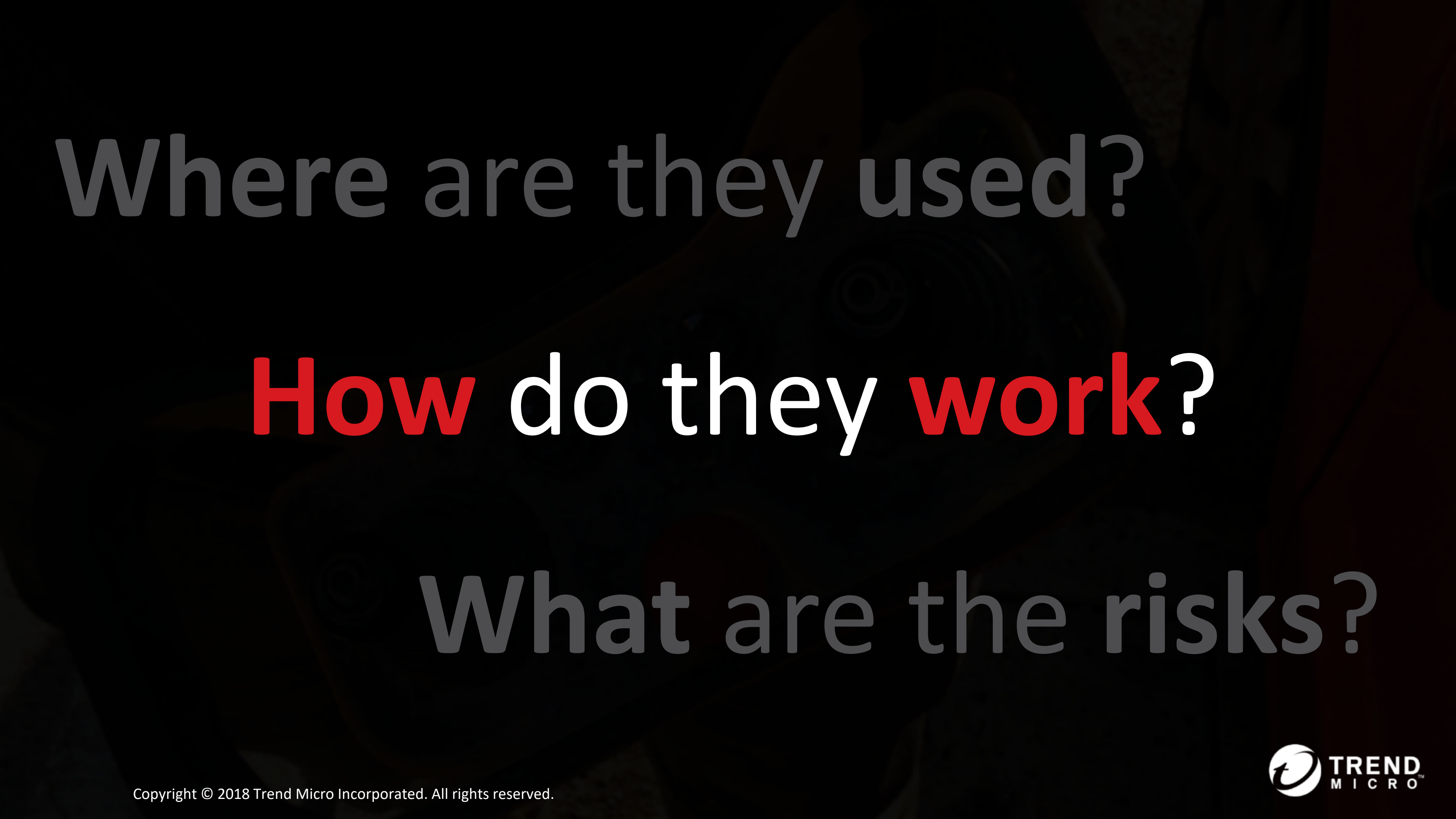
MATERIAL MINING



WORLDWIDE distribution

$1-20 MILLION annual revenue

Source : Trend Micro Research



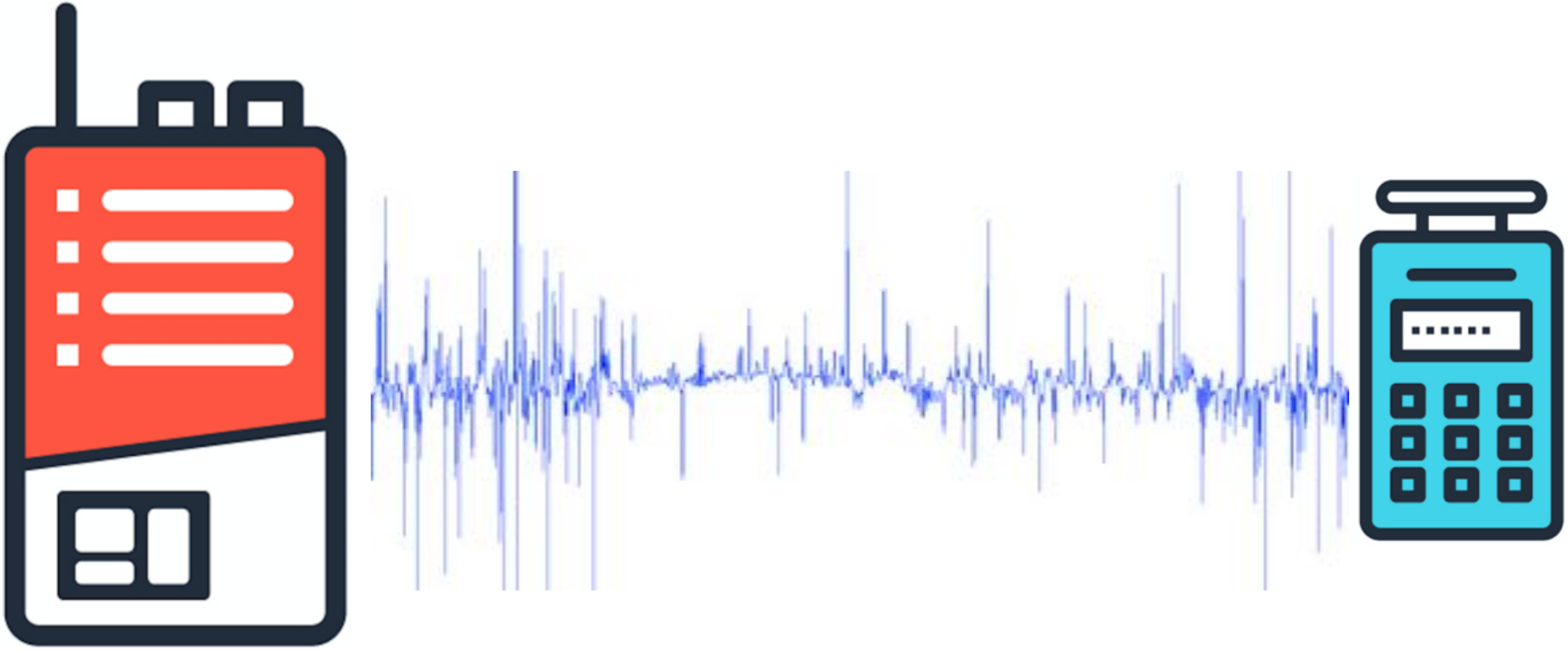
Where are they **used**?

How do they **work**?

What are the **risks**?

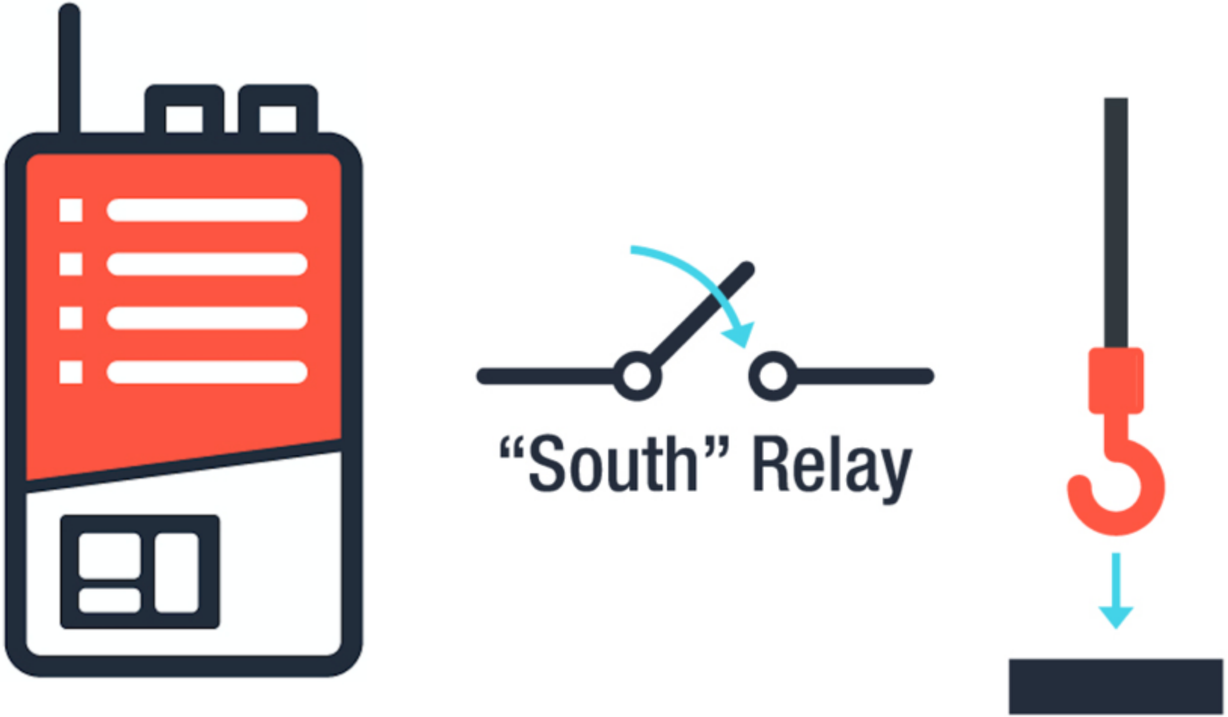
TRANSMITTER

TRANSMITTER



RECEIVER

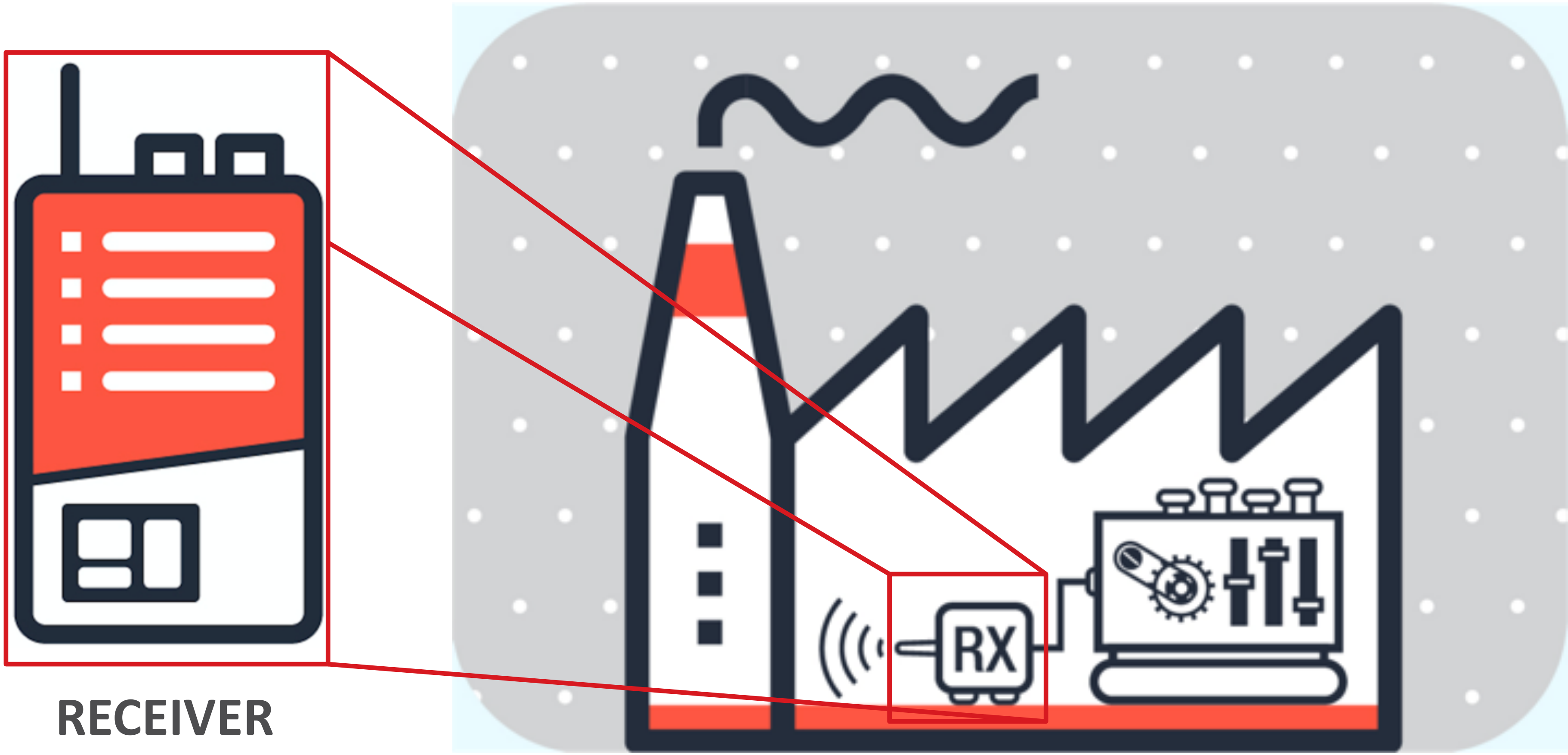
TRANSMITTER



“South” Relay

Motor Drive

RECEIVER



RECEIVER

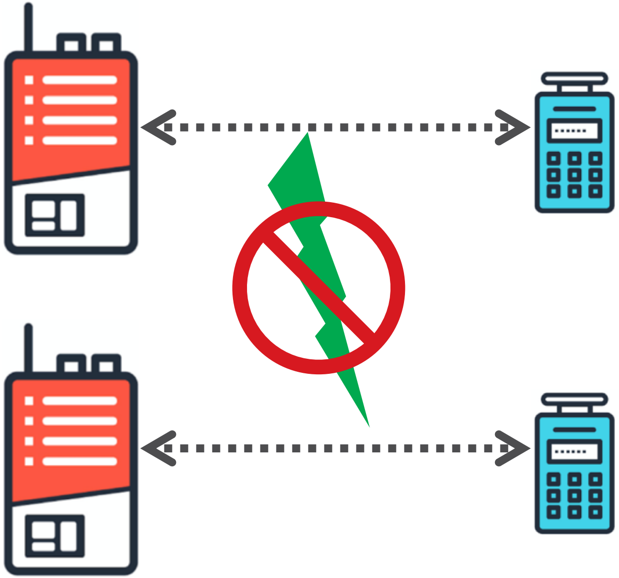
FACTORY

~~Security~~ Safety Features

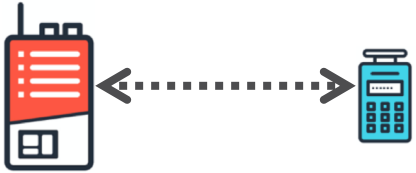
SAFETY FEATURE

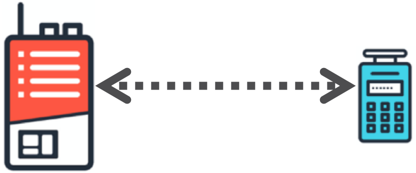
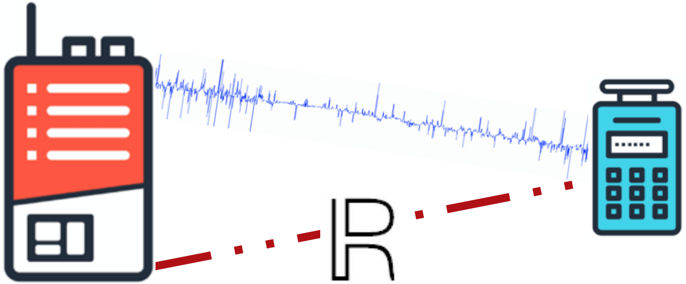
PREVENTS

Pairing Mechanism

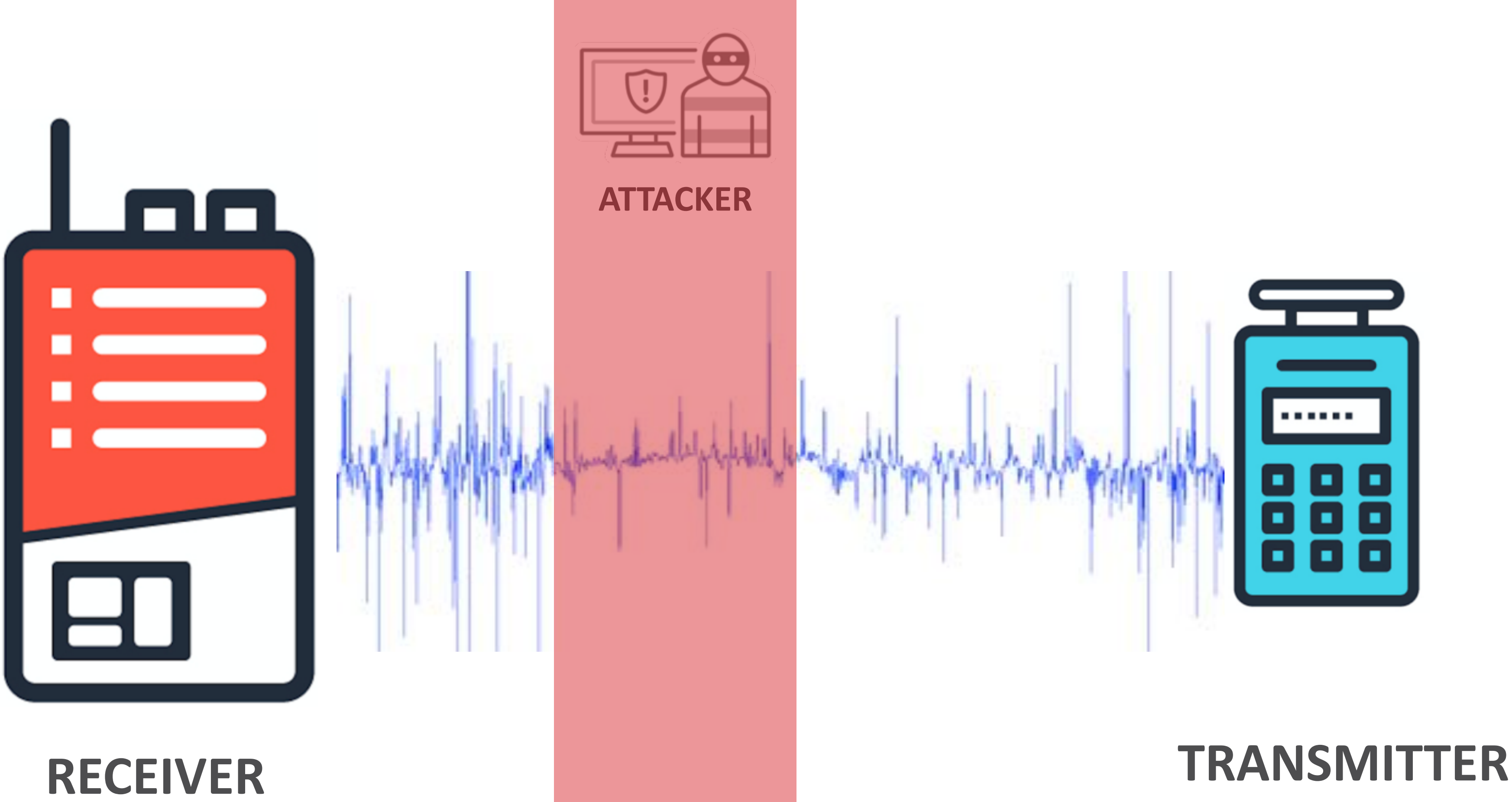


Interferences

SAFETY FEATURE	PREVENTS
Pairing Mechanism 	Interferences
Passcode Protection Passcode:**** Authorization	Unauthorized use

SAFETY FEATURE		PREVENTS
Pairing Mechanism		Interferences
Passcode Protection Authorization		Unauthorized use
Virtual Fencing		Out-of-range operation

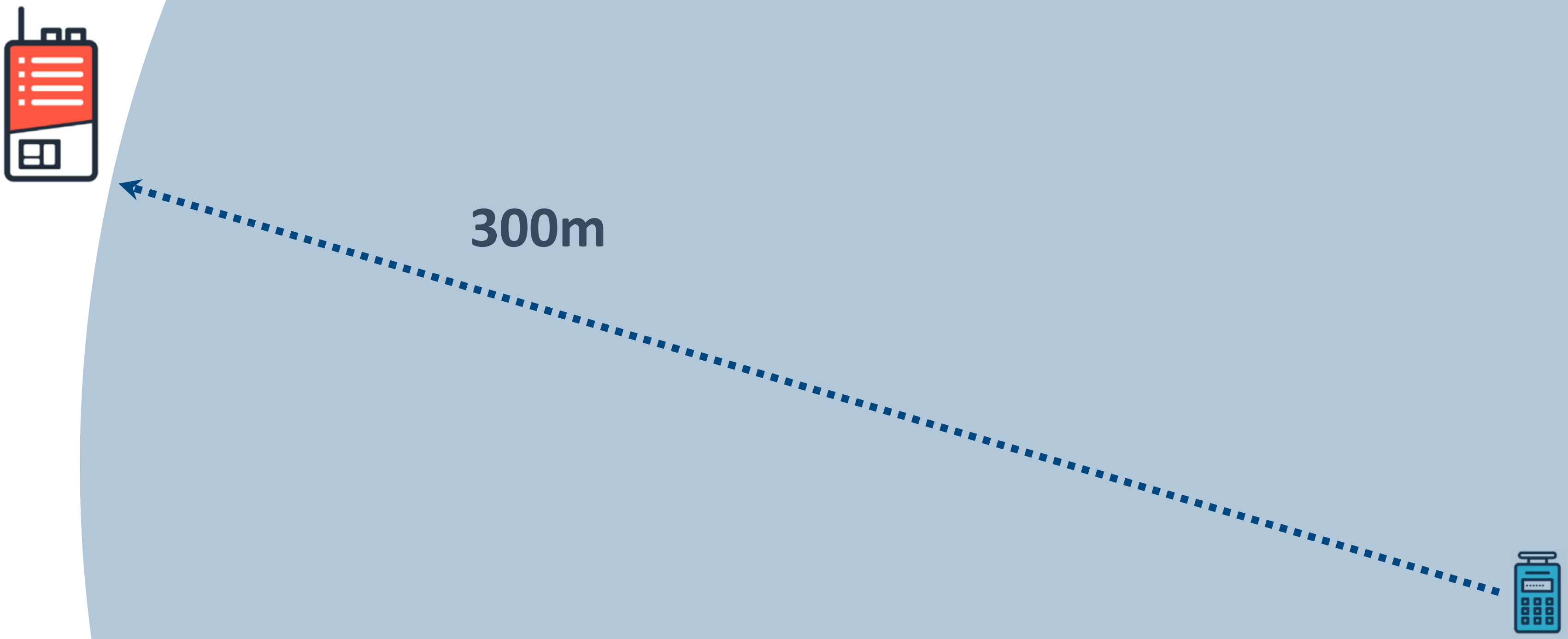
Safety	against errors
Security	against active attackers



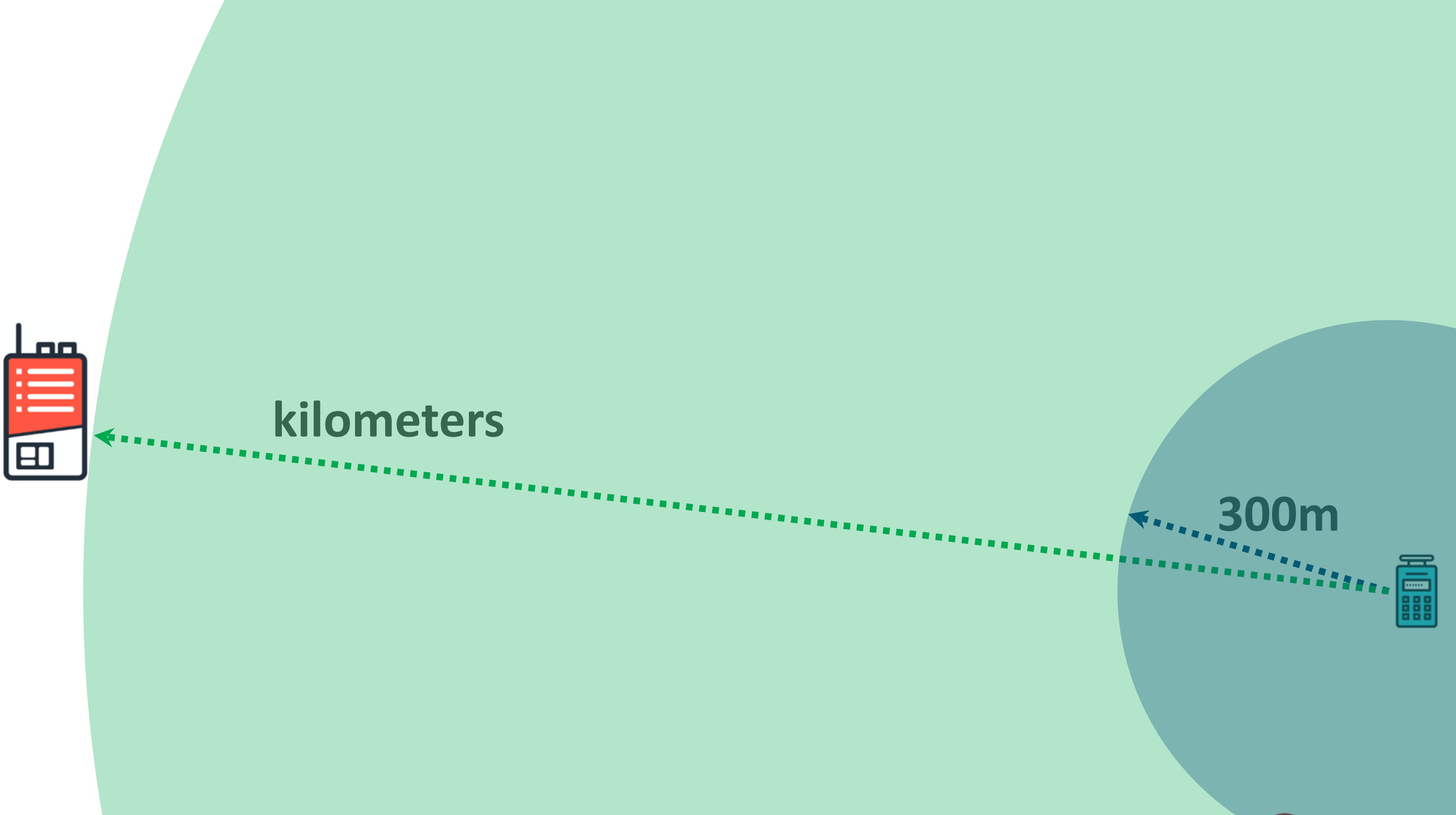
ATTACKER

RECEIVER

TRANSMITTER

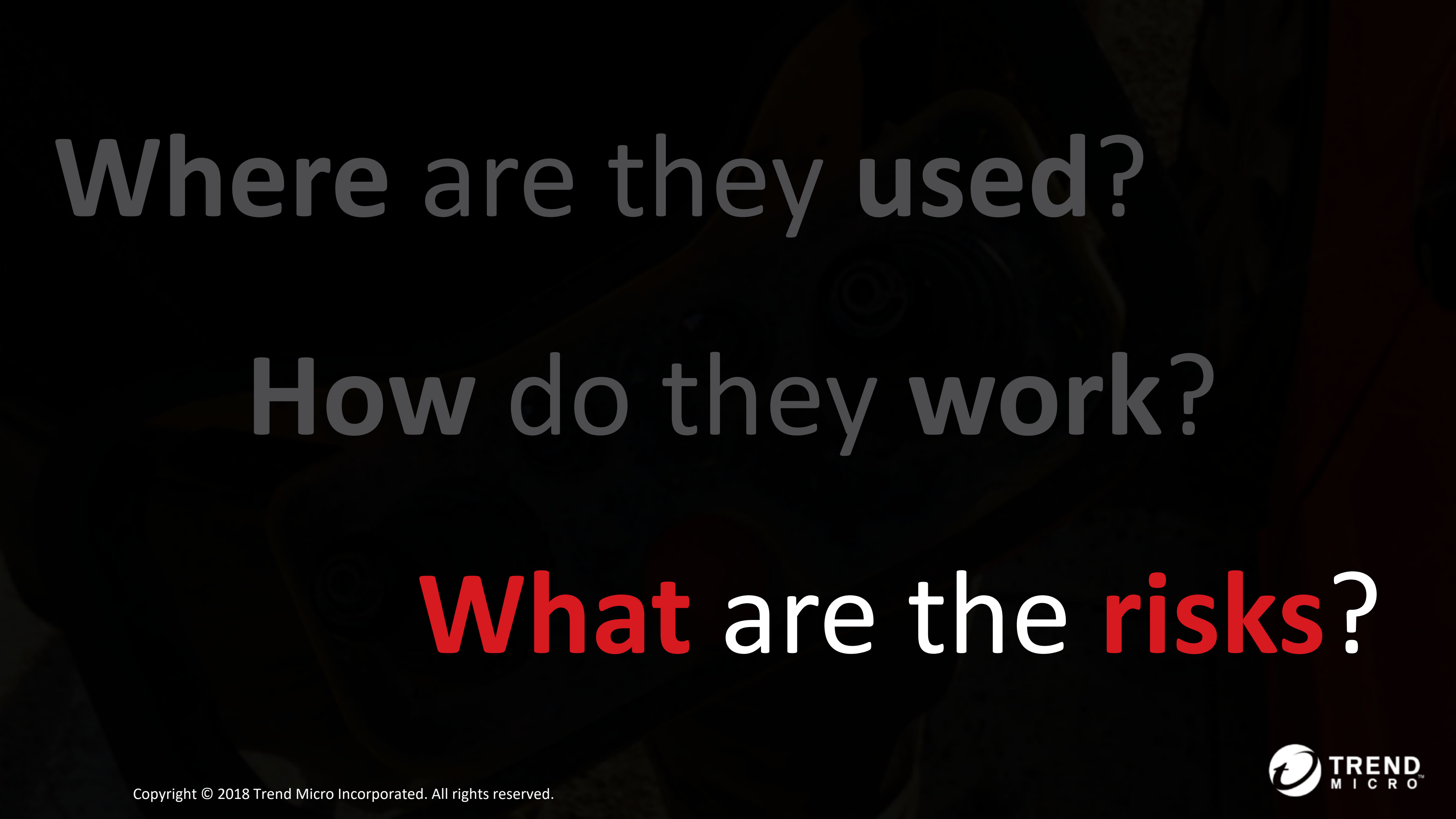


300m



kilometers

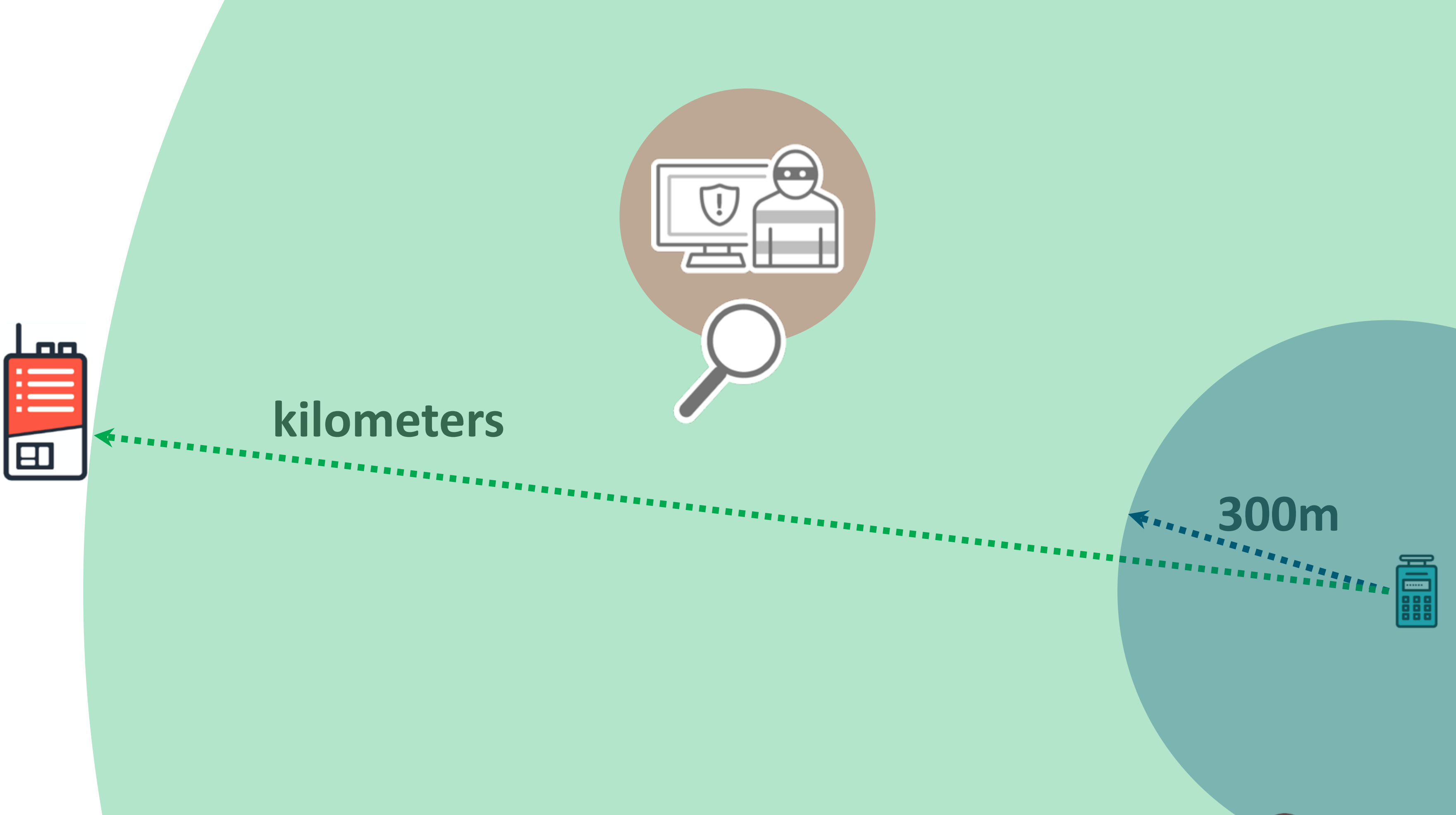
300m

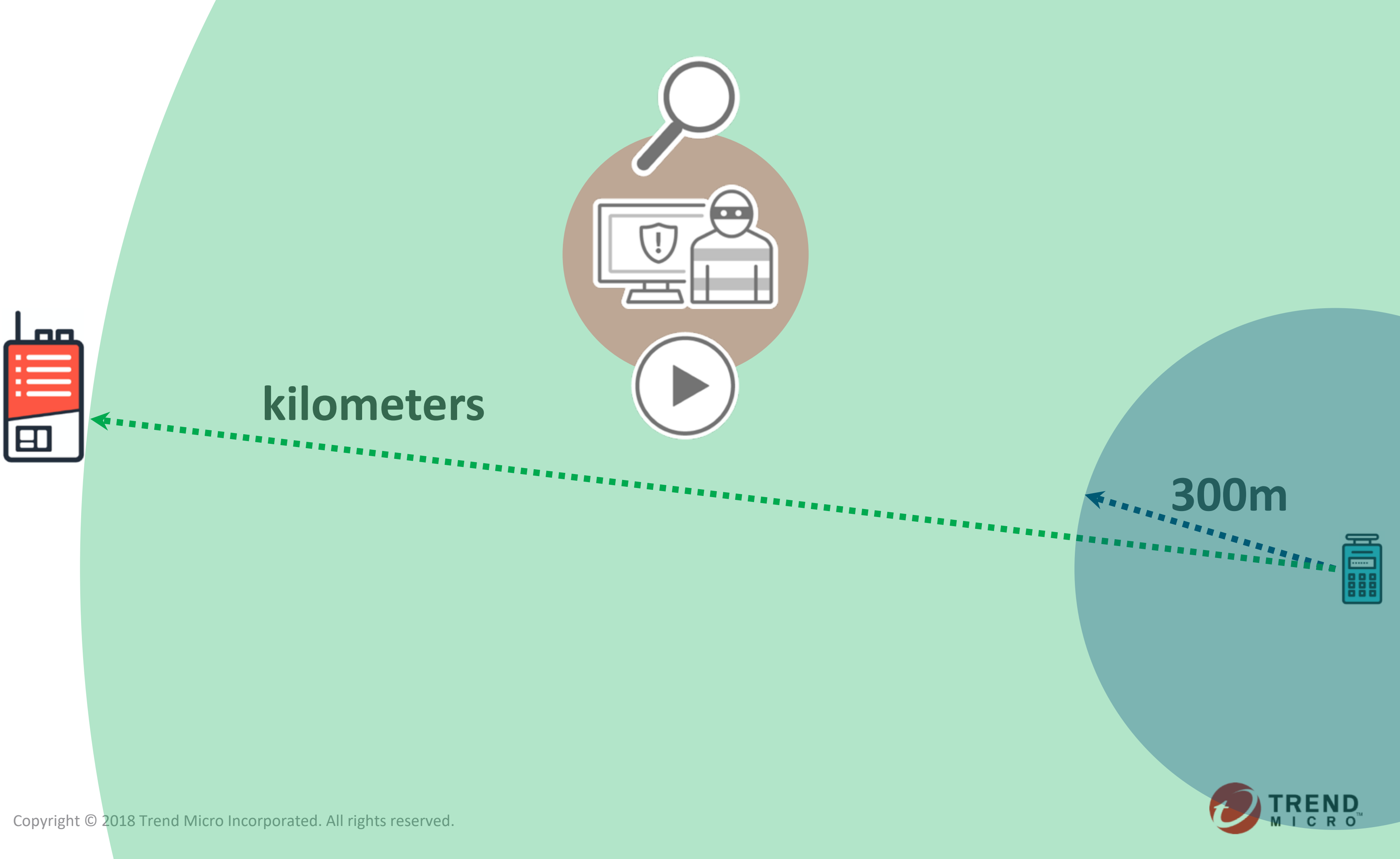


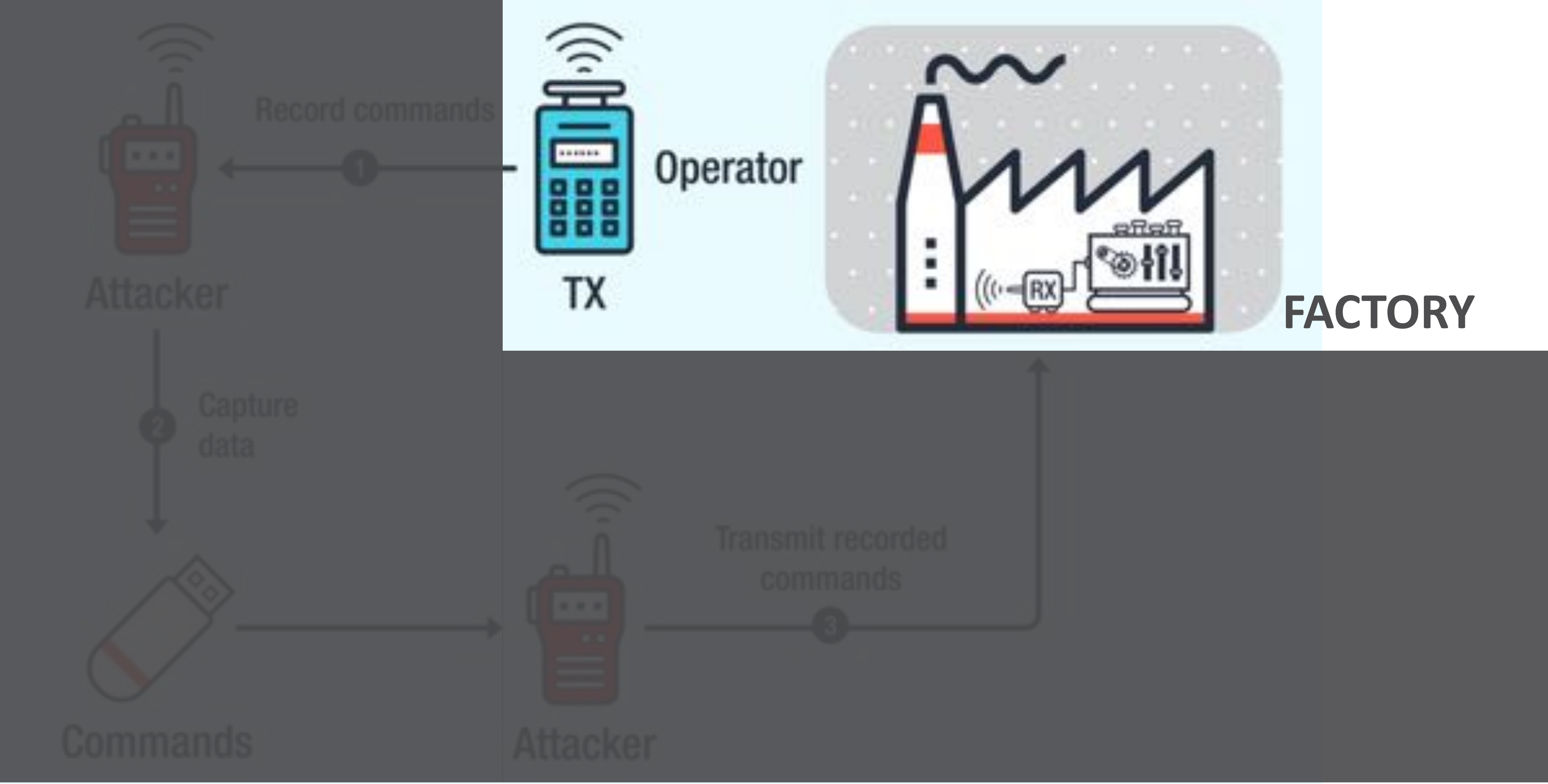
Where are they **used**?

How do they **work**?

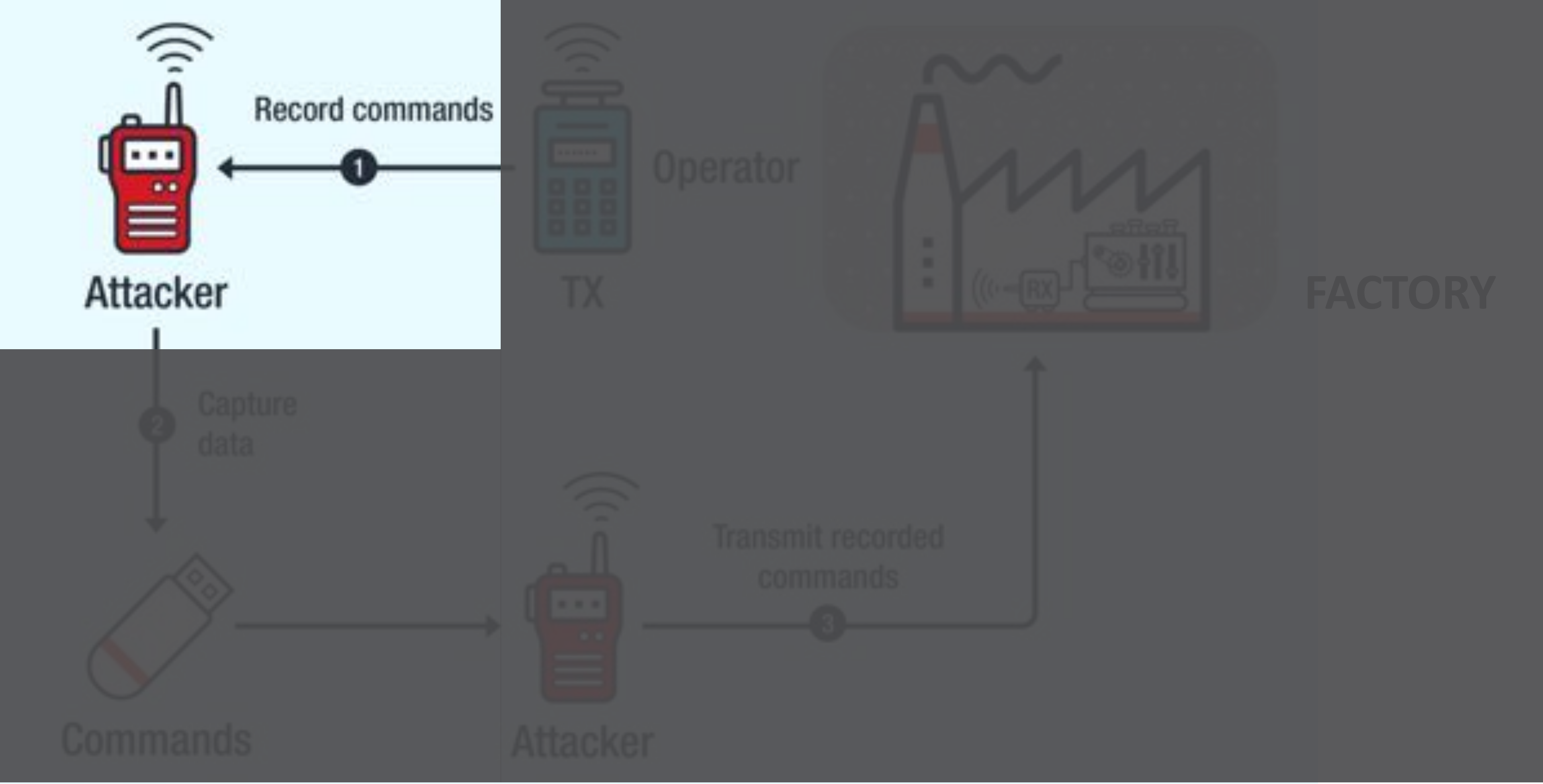
What are the **risks**?


kilometers
300m

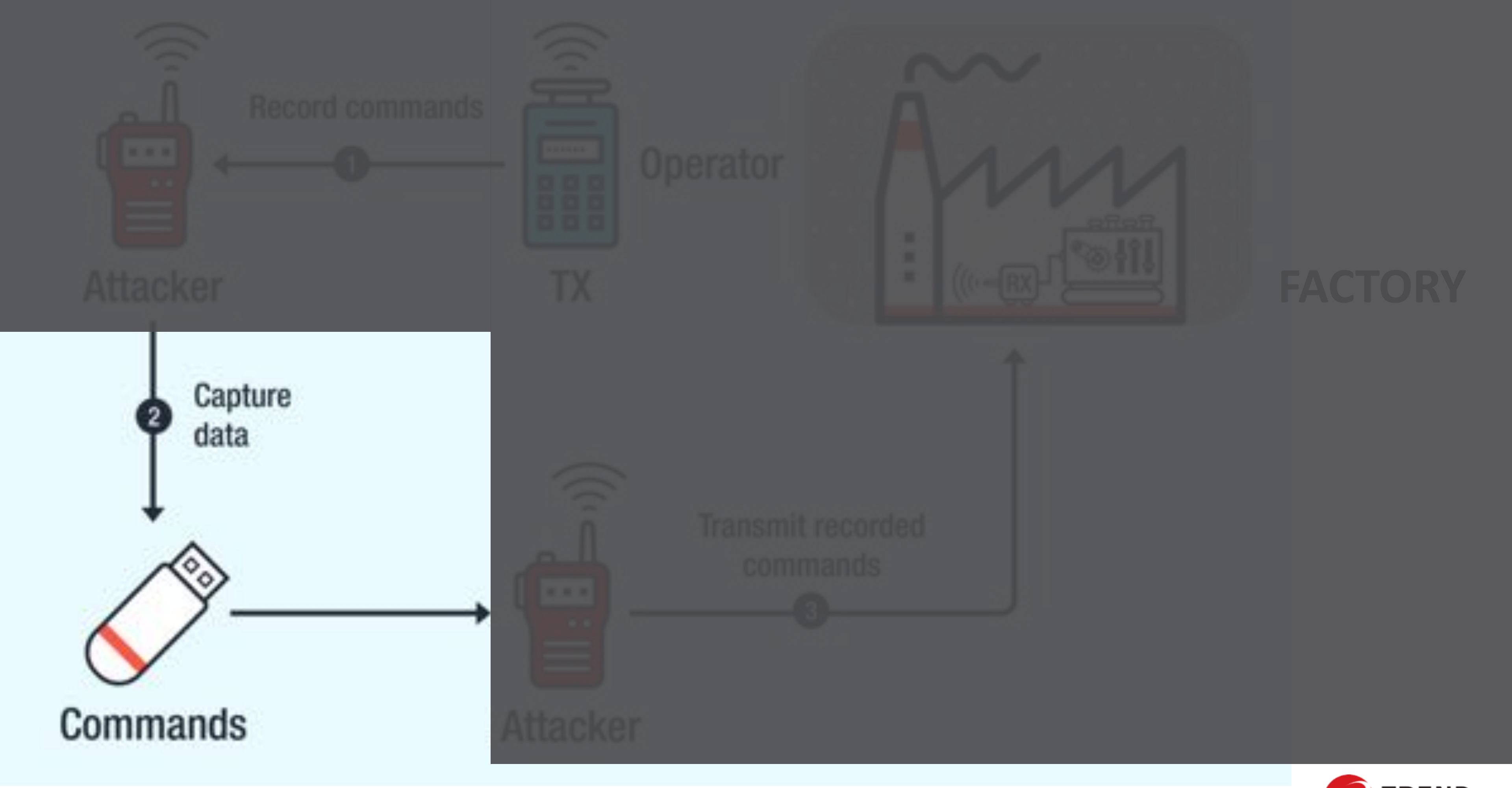

kilometers
300m

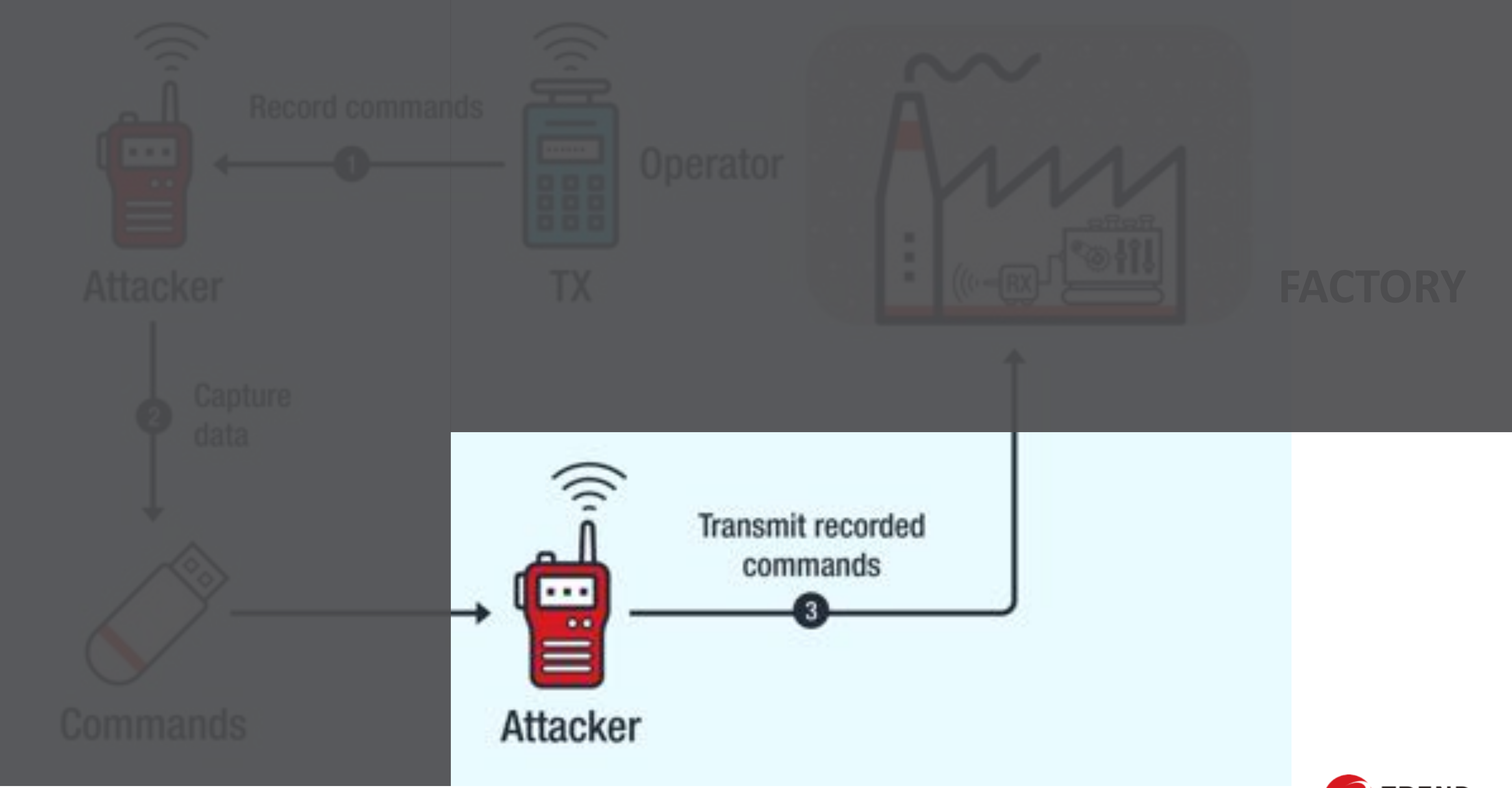

Record commands
1
Attacker
Capture
data
2
Commands
Operator
TX
RX
Attacker
Transmit recorded
commands
3

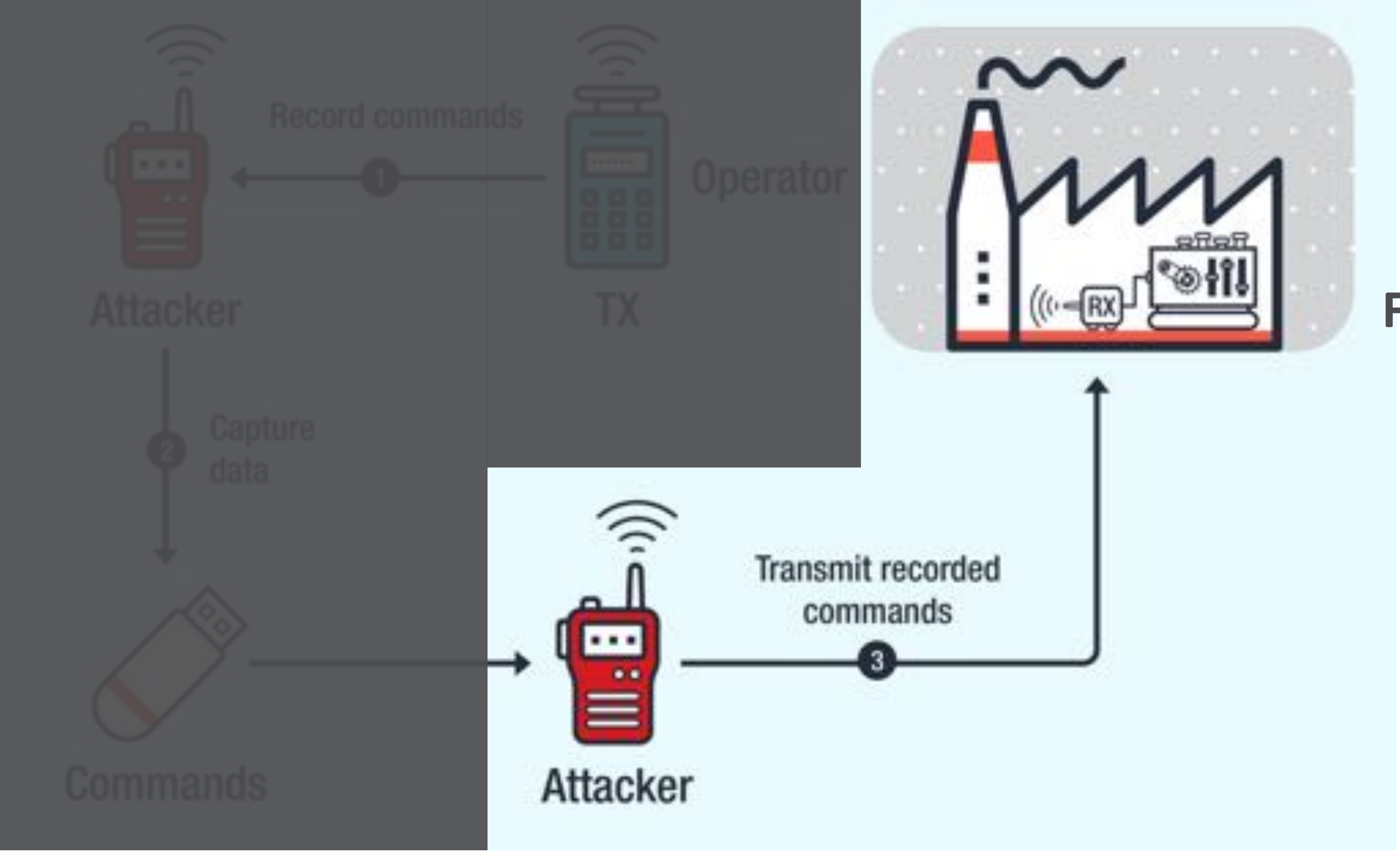
FACTORY



Record commands
1
Attacker
Operator
TX
FACTORY
RX
Capture data
2
Commands
Transmit recorded commands
3
Attacker


Record commands
1
Attacker
TX
Operator
RX
FACTORY
2
Capture data
Commands
Transmit recorded commands
3
Attacker


Record commands
1
Attacker
Operator
TX
FACTORY
RX
Capture
data
2
Commands
Transmit recorded
commands
3
Attacker


Record commands
1
Operator
Attacker
TX
Capture data
2
Commands
Transmit recorded commands
3
Attacker
RX

FACTORY

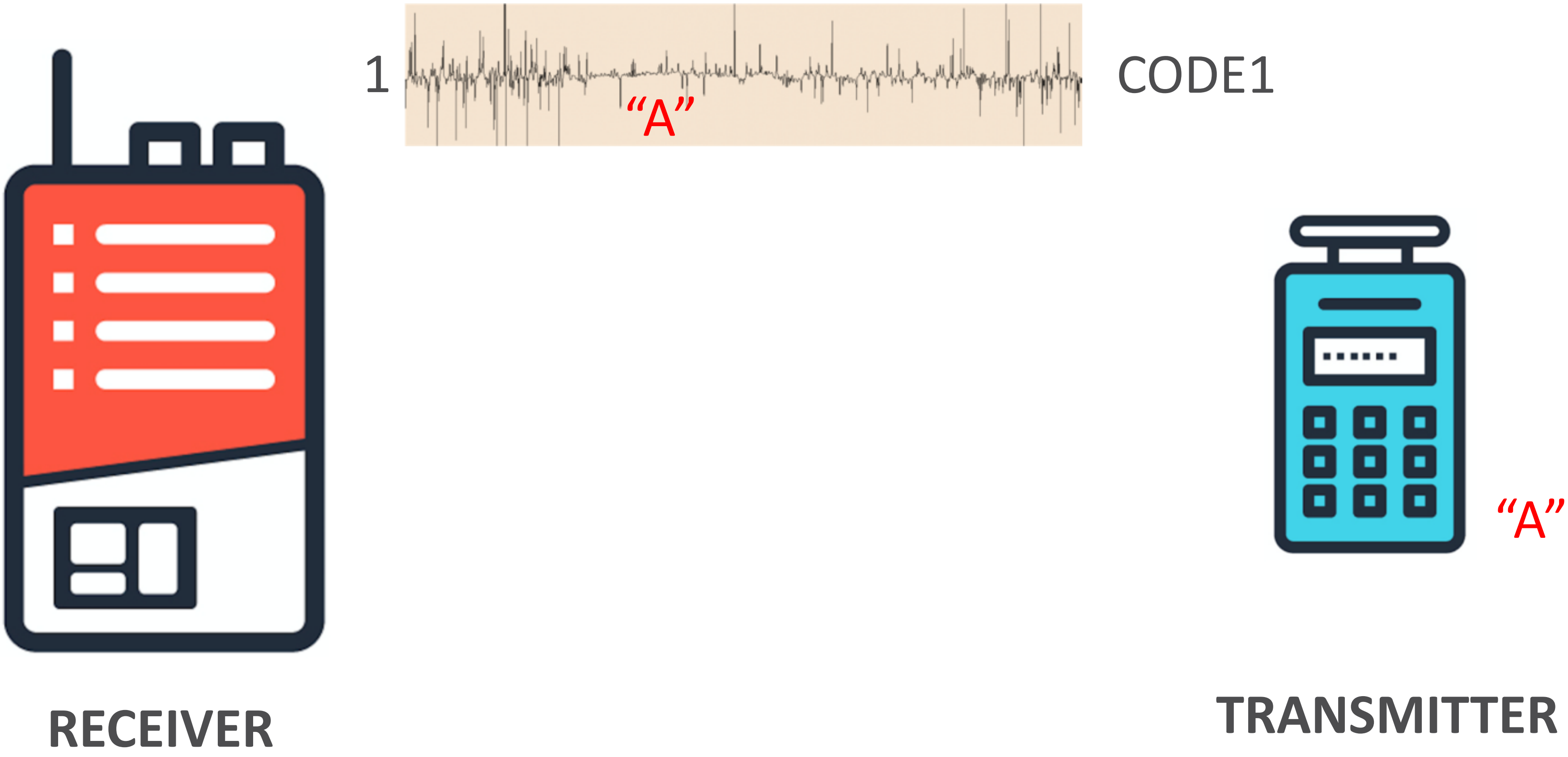
Are replay attacks easy?

Are replay attacks easy?

They should not!

RECEIVER

TRANSMITTER



1

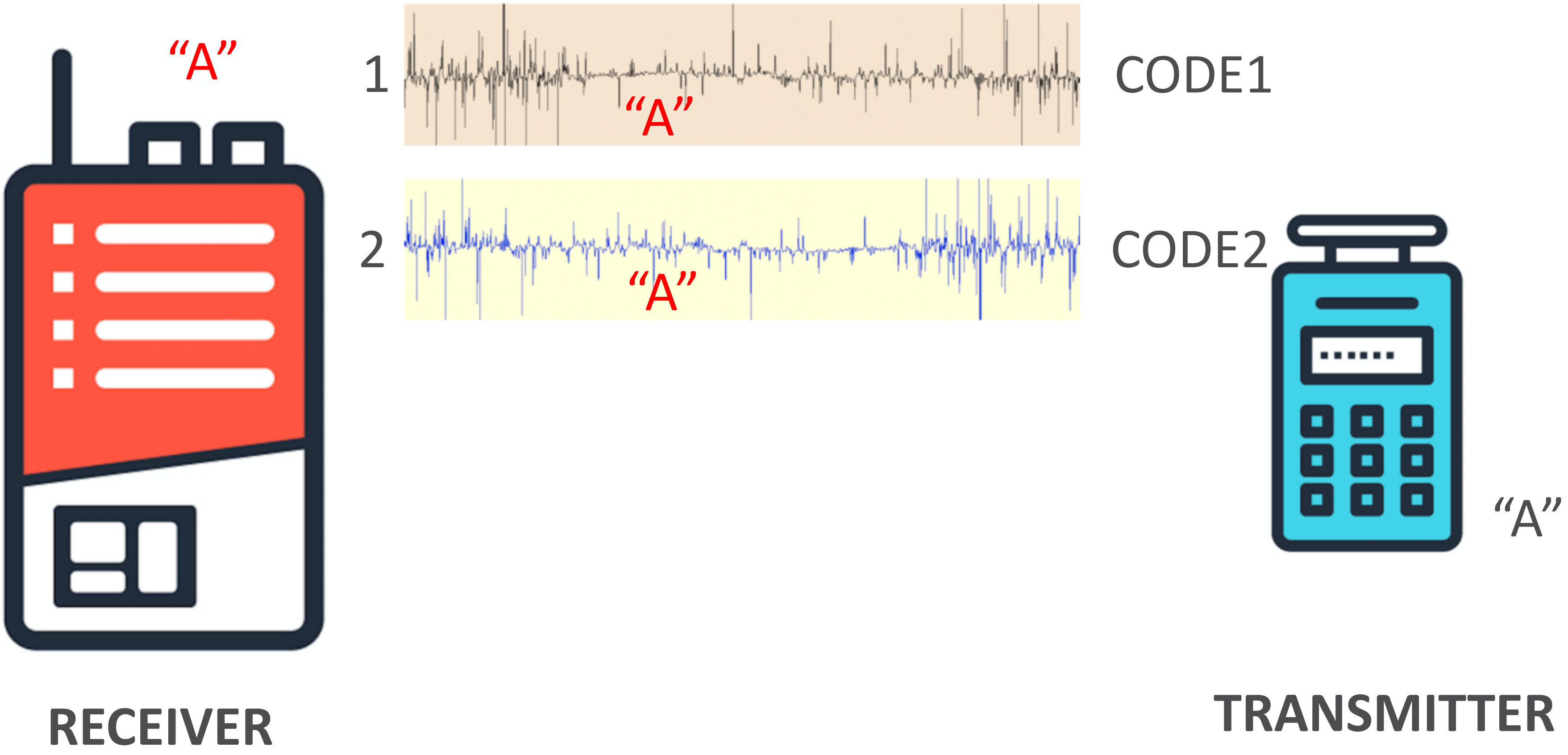
“A”

CODE1

“A”

RECEIVER

TRANSMITTER



“A”

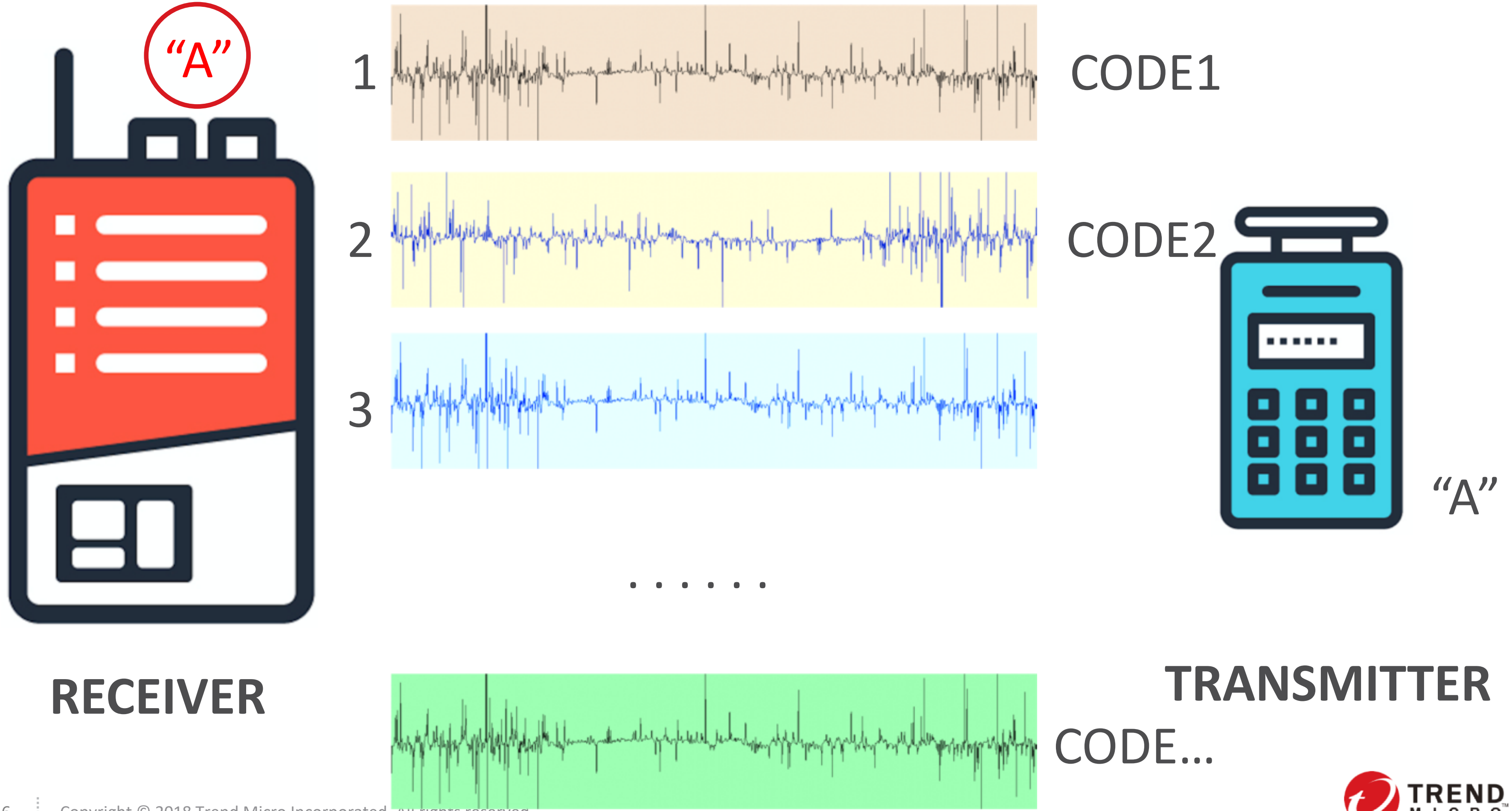
1 “A” CODE1

2 “A” CODE2

“A”

RECEIVER

TRANSMITTER



“A”

1

CODE1

2

CODE2

3

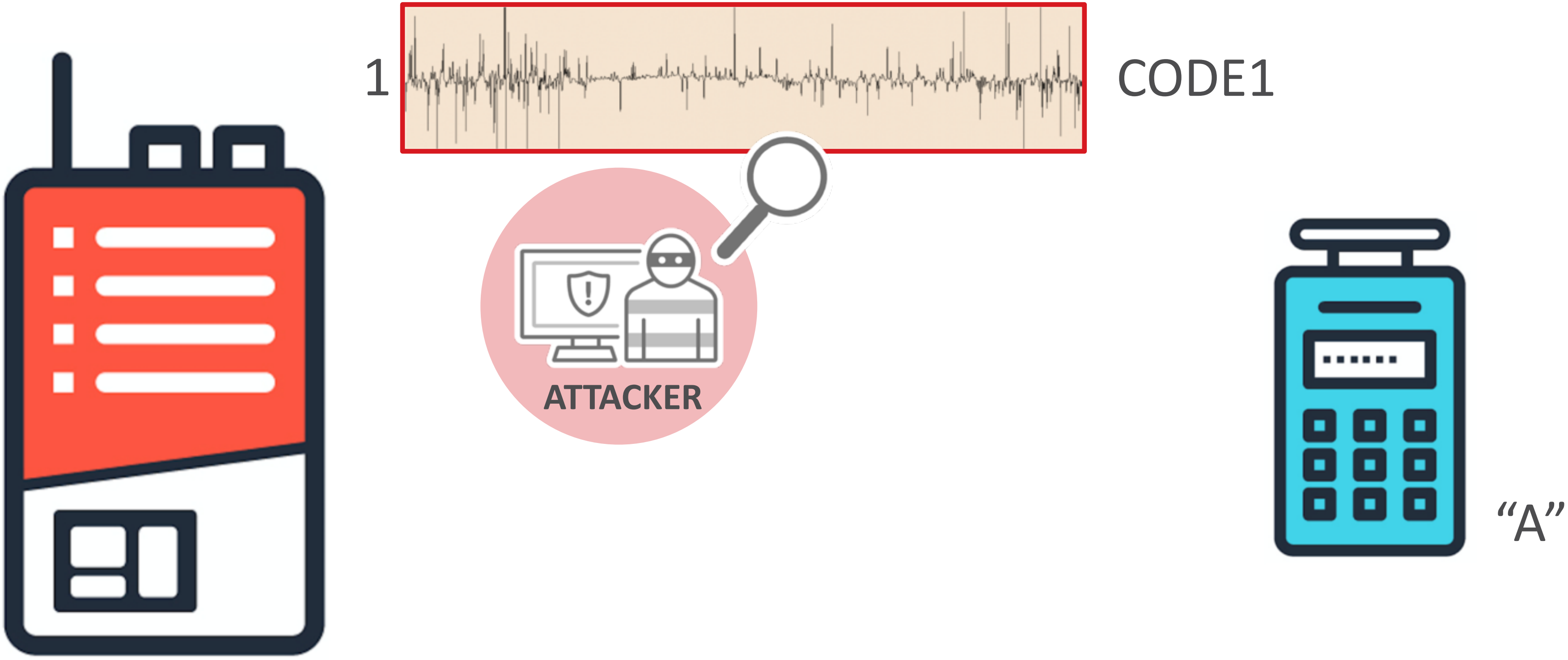
“A”

. . . . . .

RECEIVER

TRANSMITTER

CODE…



1

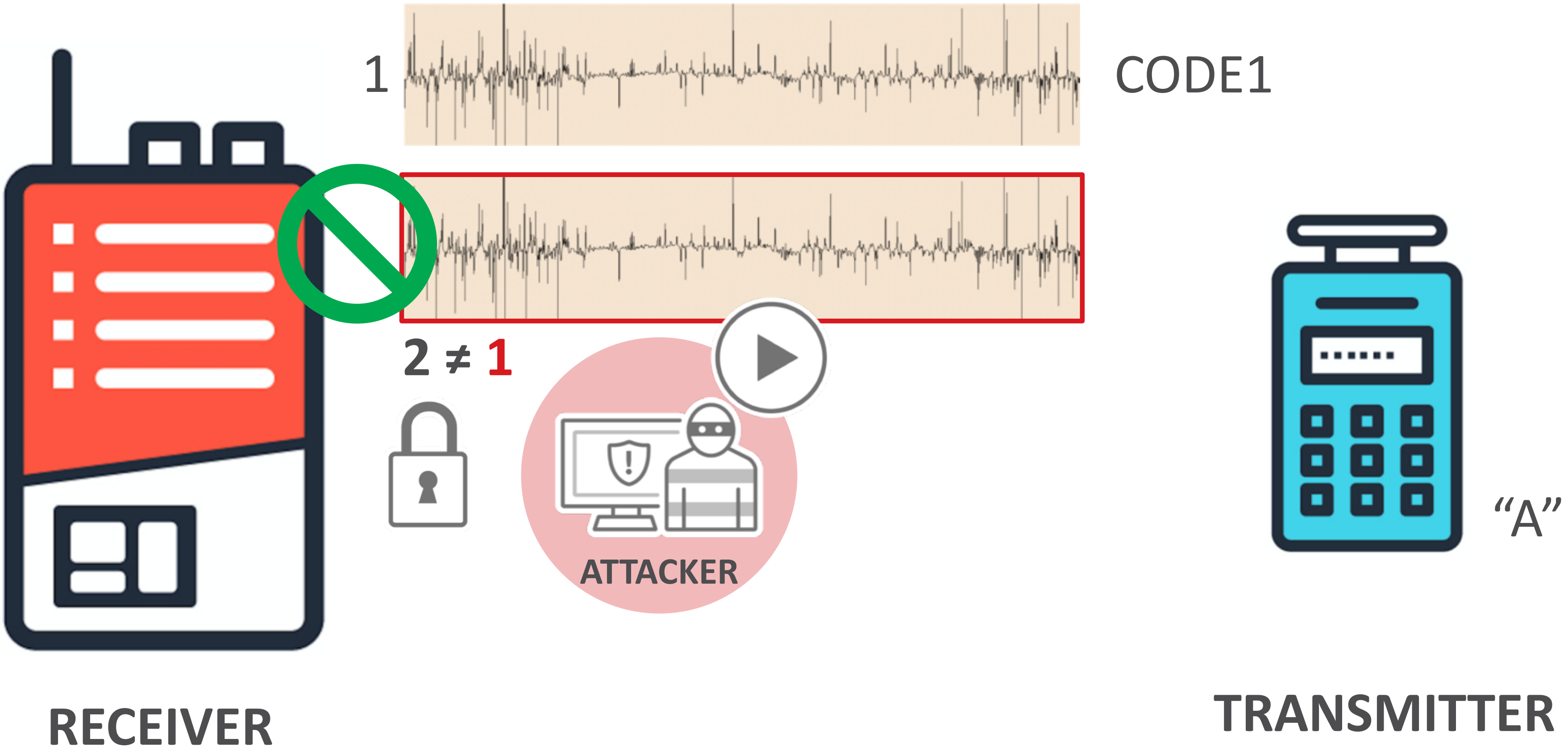
CODE1

ATTACKER

“A”

RECEIVER

TRANSMITTER



1

CODE1

2 ≠ 1

ATTACKER

“A”

RECEIVER

TRANSMITTER

Are replay attacks

EXPENSIVE?

100% HARDWARE

$480

$299

SOFTWARE-DEFINED RADIOs

$99

RADIO-HACKING DONGLEs

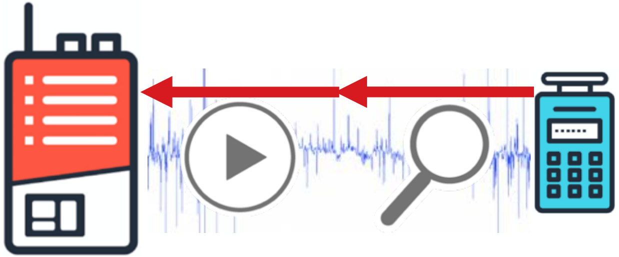
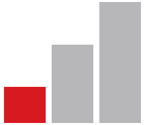
$480

$299

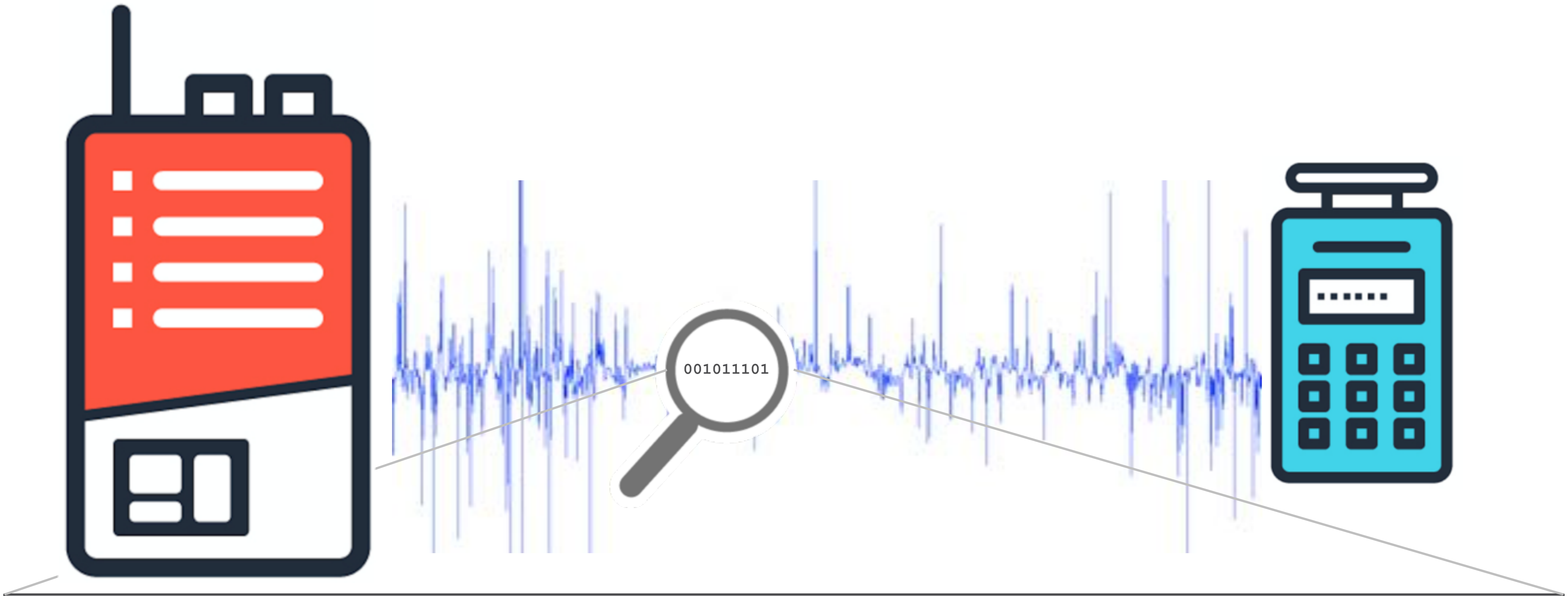
$99

LOWER BARRIER

A SECURITY ANALYSIS OF
RADIO REMOTE CONTROLLERS
FOR INDUSTRIAL APPLICATIONS

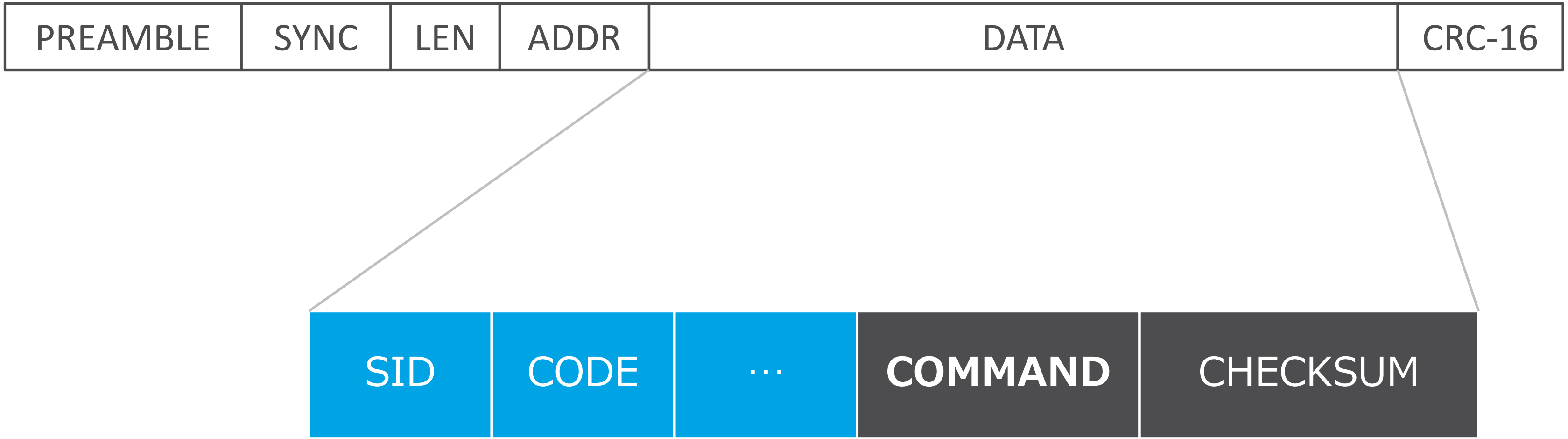
ATTACK CLASS	Vendors	Difficulty	Resources
1: Replay Attack 	All tested		$$$$

Clever attackers



1010101010101010101010 1001001100001011 101000111011110 00001101 10100010 11110101…

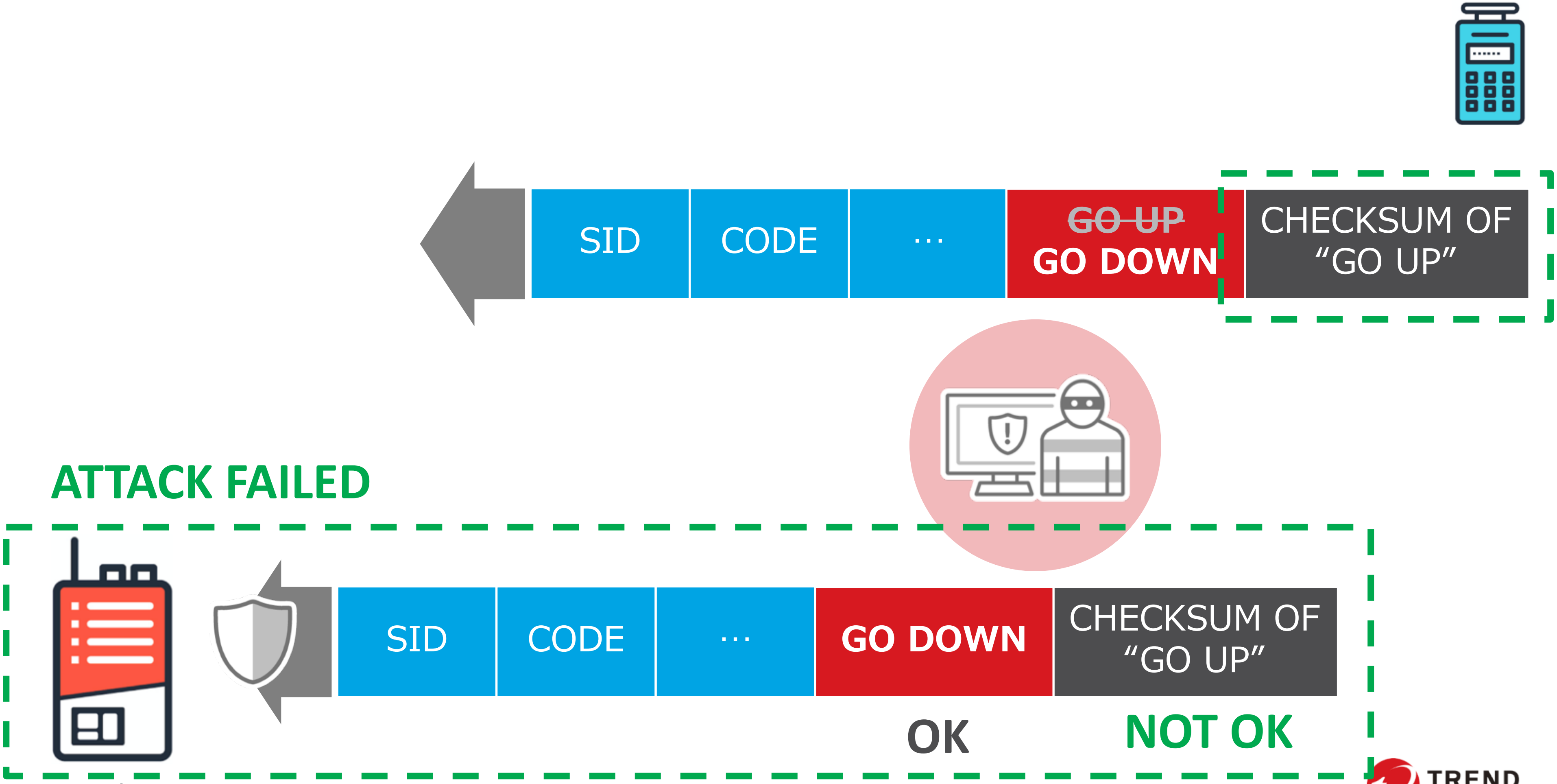
101010101010101010101010 1001001100001011 1010001110111110 00001101 10100010 11110101…



PREAMBLE | SYNC | LEN | ADDR | DATA | CRC-16

SID | CODE | … | **COMMAND** | CHECKSUM

ATTACK FAILED



SID

CODE

…

~~GO UP~~

GO DOWN

CHECKSUM OF “GO UP”

SID

CODE

…

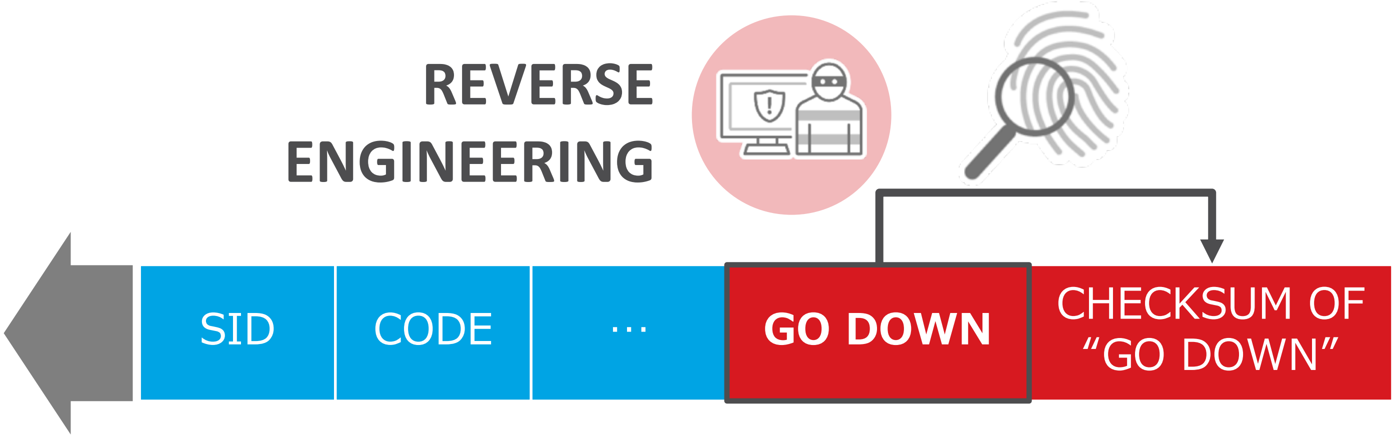
GO DOWN

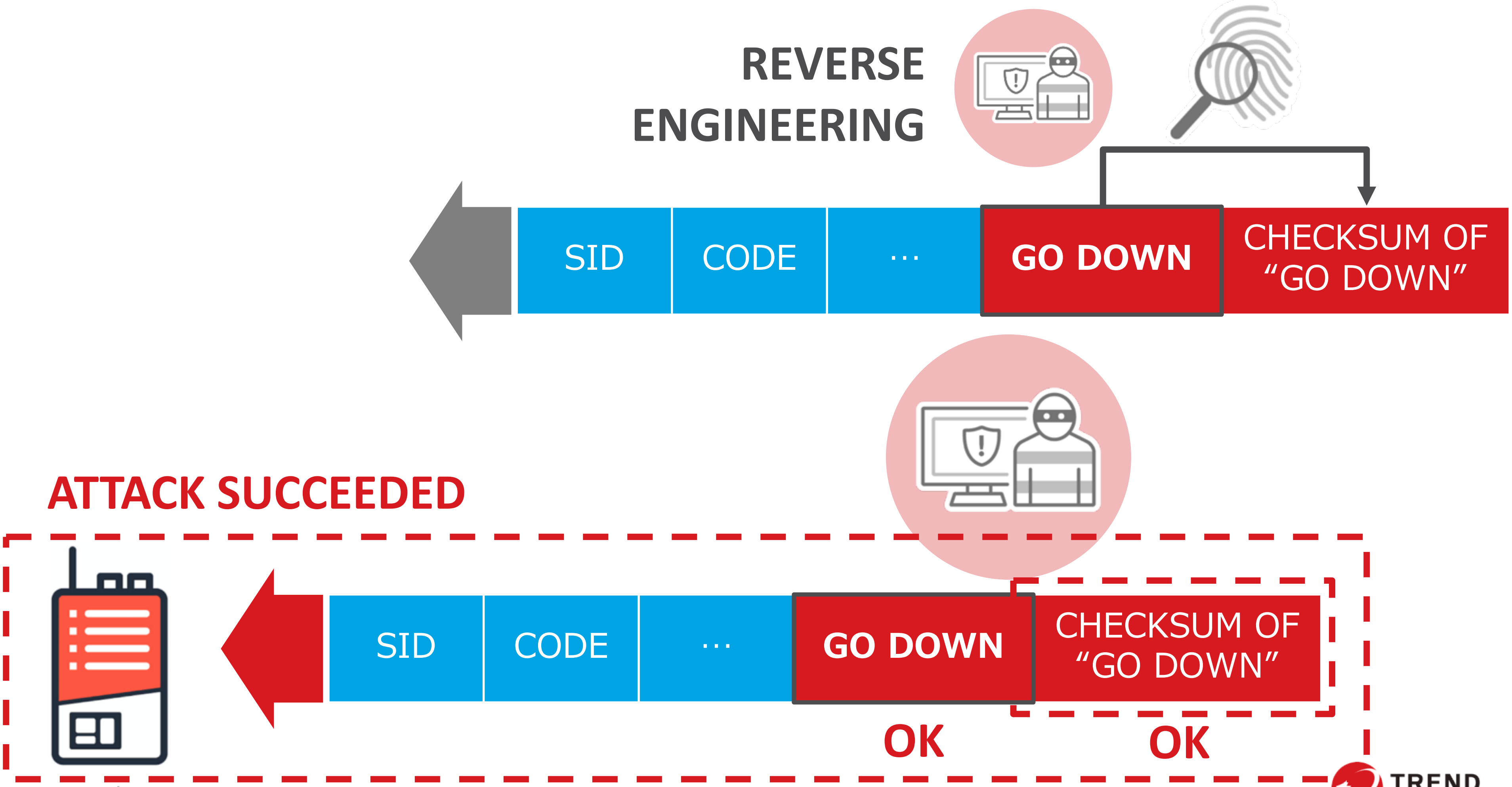
CHECKSUM OF “GO UP”

OK

NOT OK

REVERSE ENGINEERING





REVERSE ENGINEERING

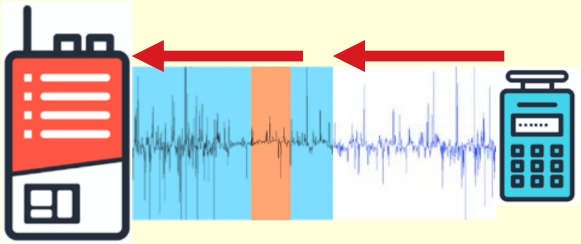
SID | CODE | … | GO DOWN | CHECKSUM OF "GO DOWN"

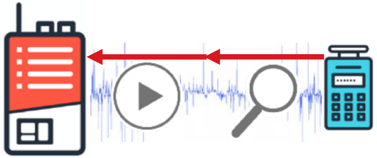
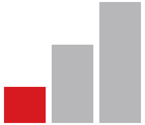
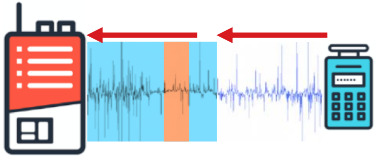
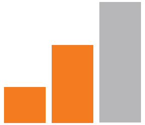
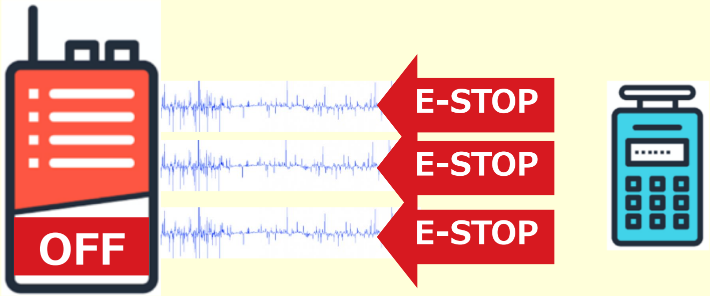
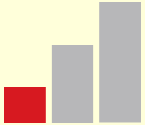
ATTACK SUCCEEDED

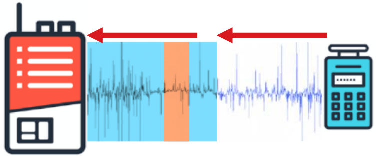
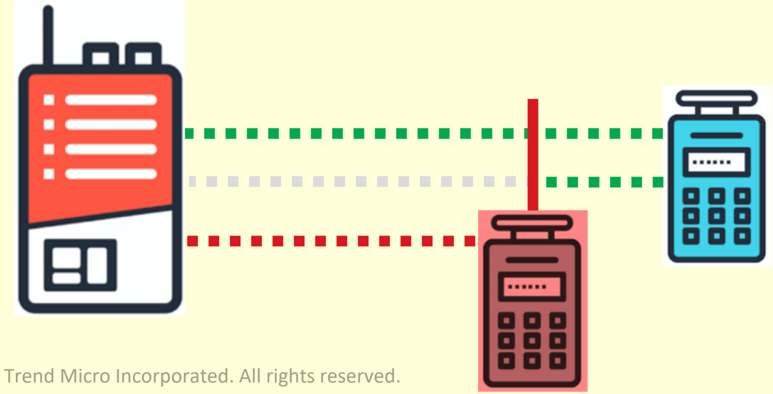
SID | CODE | … | GO DOWN | CHECKSUM OF "GO DOWN"

OK

OK

ATTACK CLASS		Vendors	Difficulty	Resources
1: Replay Attack		All tested	■□□	$$$$
2: Command Injection		All tested	■■□	$$$$

ATTACK CLASS		Vendors	Difficulty	Resources
1: Replay Attack		All tested		$$$$
2: Command Injection		All tested		$$$$
3: E-Stop Abuse		All tested		$$$$

ATTACK CLASS	Vendors	Difficulty	Resources
1: Replay Attack 	All tested	🟥 ▮ ▮	**$**$$$
2: Command Injection 	All tested	🟧 🟧 ▮	**$$**$$
3: E-Stop Abuse OFF E-STOP E-STOP E-STOP	All tested	🟥 ▮ ▮	**$**$$$
4: Malicious Re-pairing 	Some of tested	🟧 🟧 ▮	**$$**$$

Short-range attackers

vs

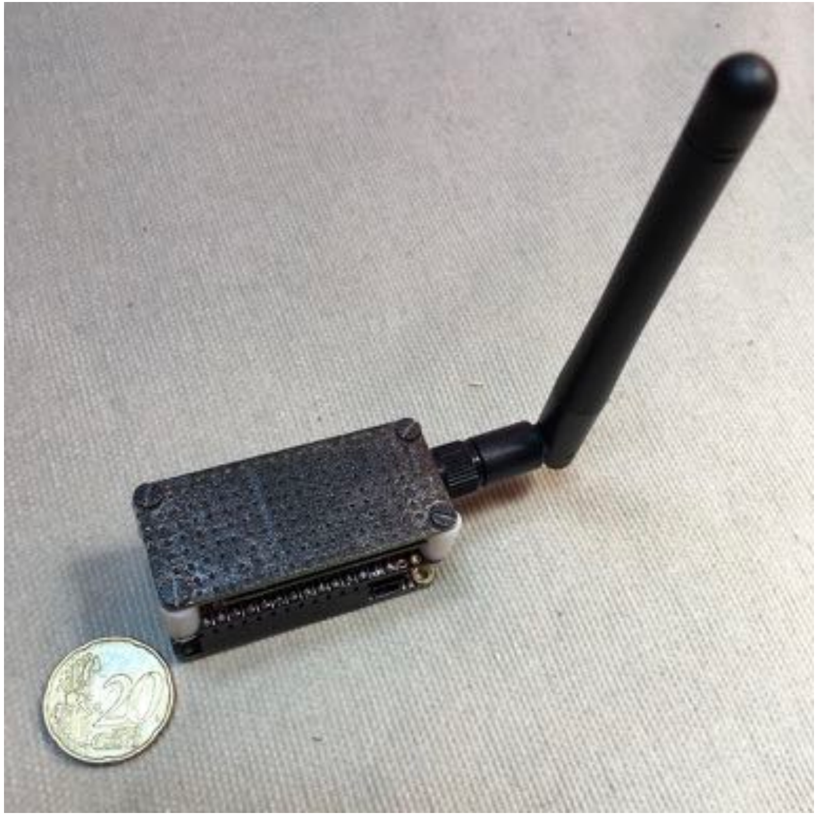
Internet attackers

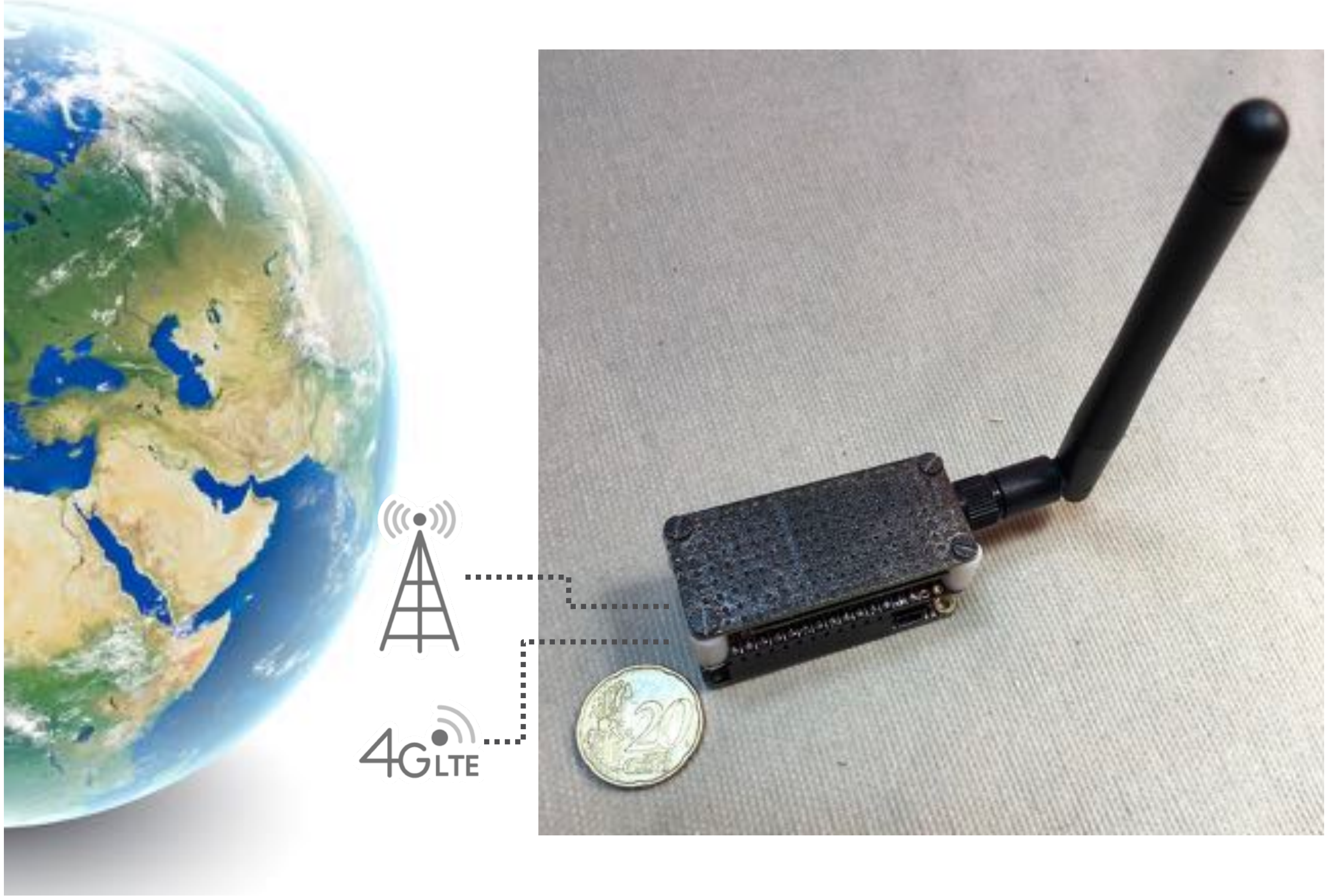
Short-range attackers

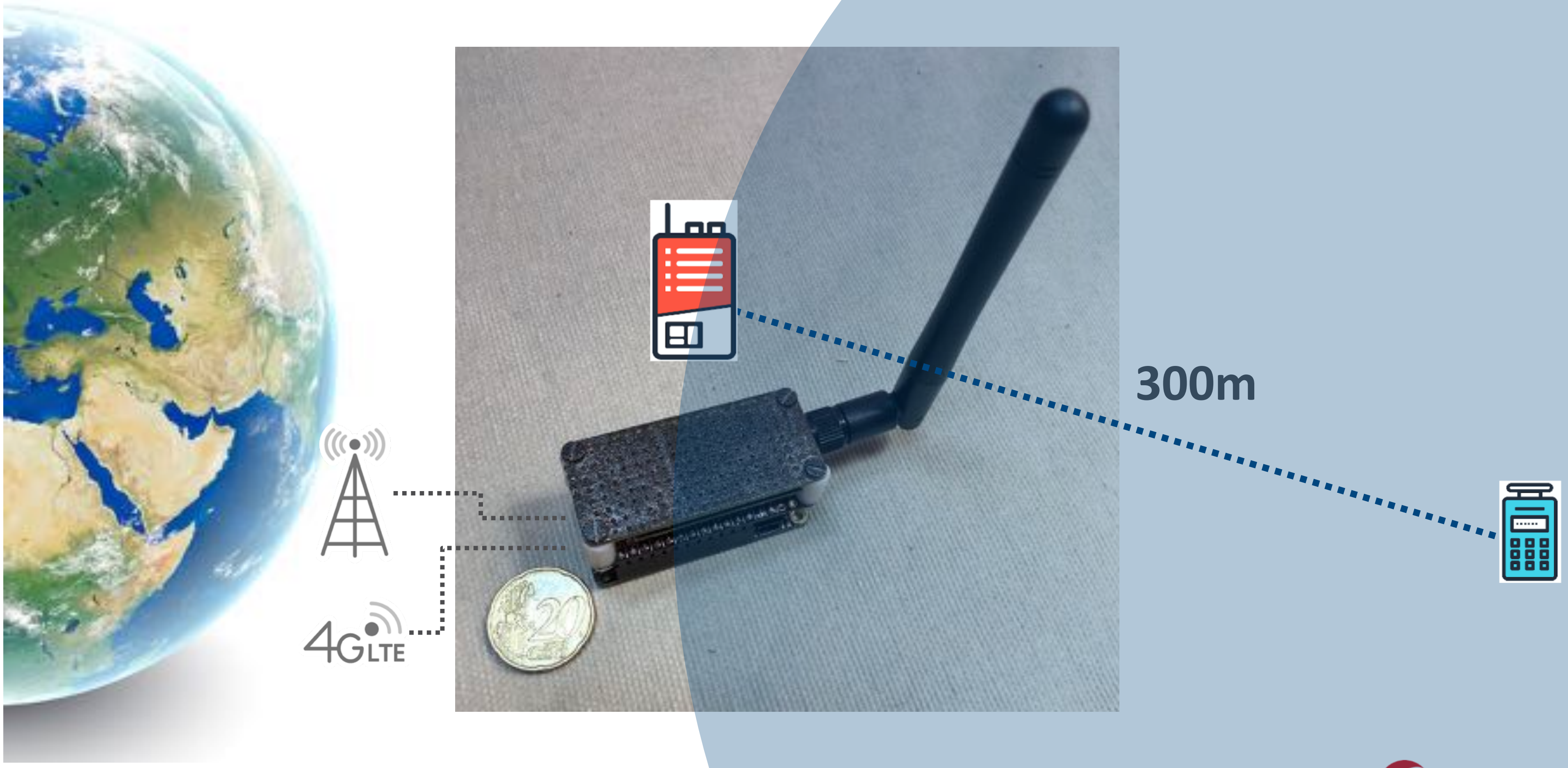
1

vs

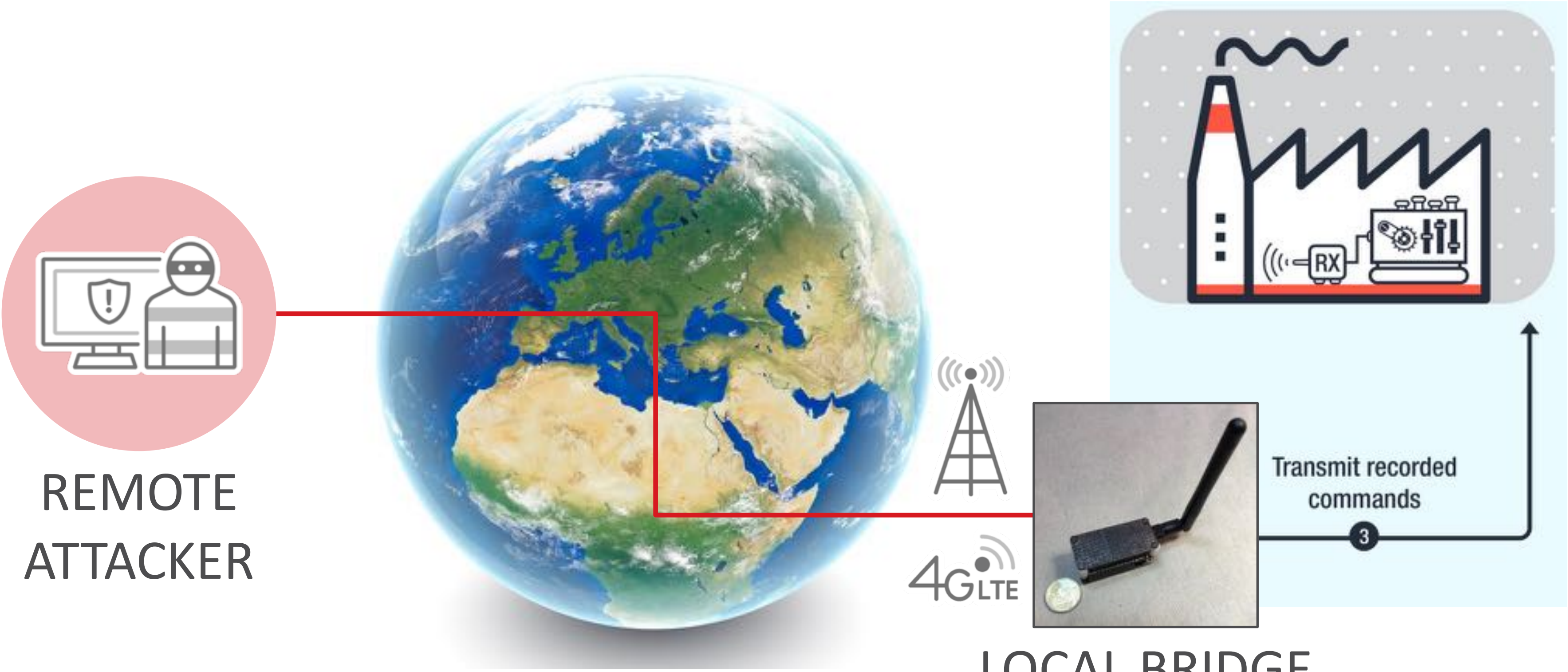
Internet attackers




4G LTE


4G LTE
300m

TARGET



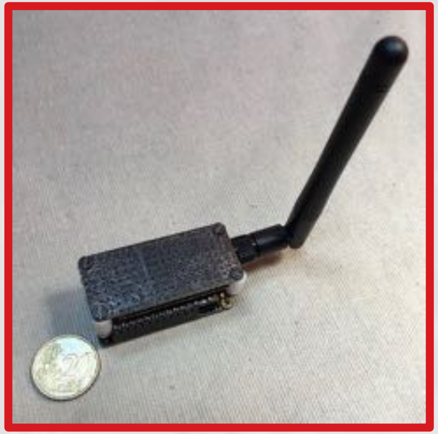
REMOTE ATTACKER

LOCAL BRIDGE

$480

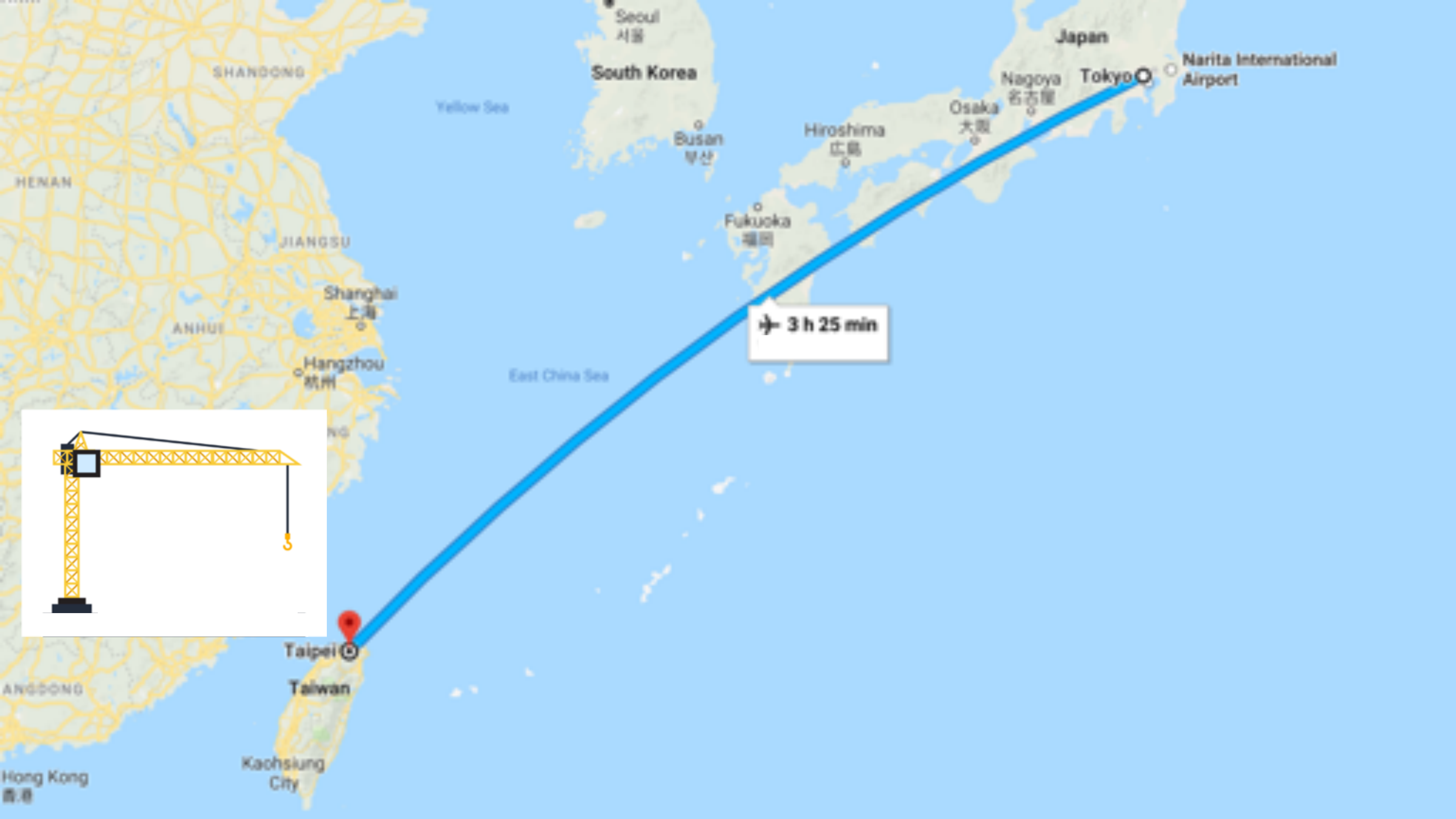
$299

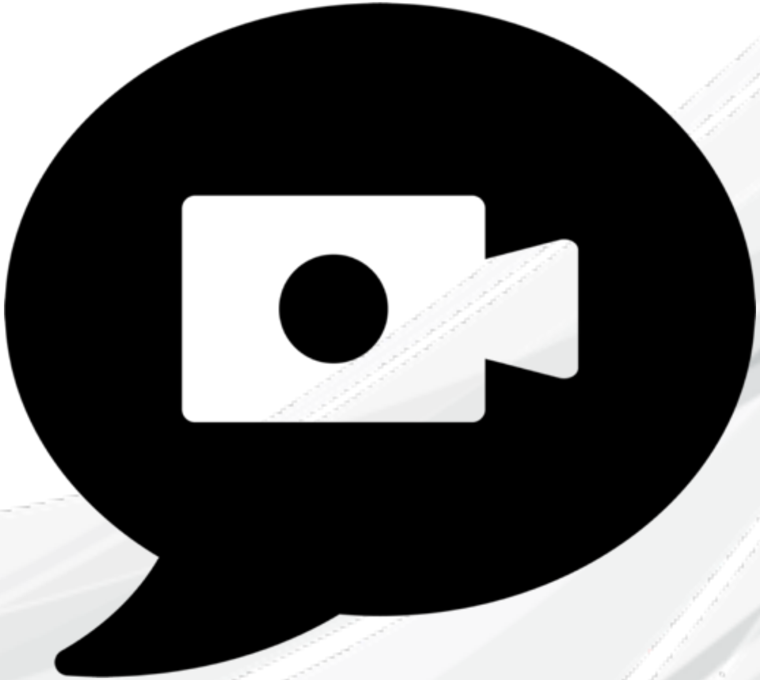
$99



$40

EVEN LOWER BARRIER

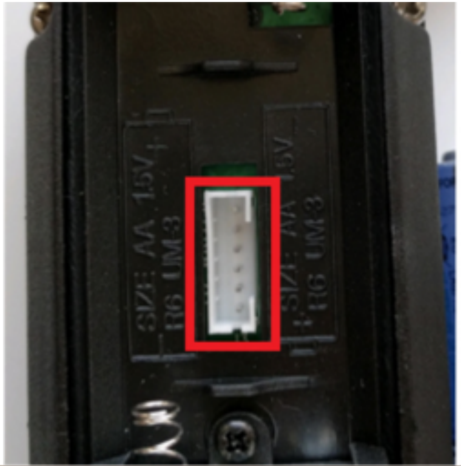

Seoul
서울
South Korea
Japan
Narita International Airport
Tokyo
Nagoya
名古屋
Osaka
大阪
Hiroshima
広島
Busan
부산
SHANDONG
Yellow Sea
HENAN
JIANGSU
Fukuoka
福岡
Shanghai
上海
ANHUI
Hangzhou
杭州
3 h 25 min
East China Sea
Taipei
Taiwan
Kaohsiung City
Hong Kong
香港

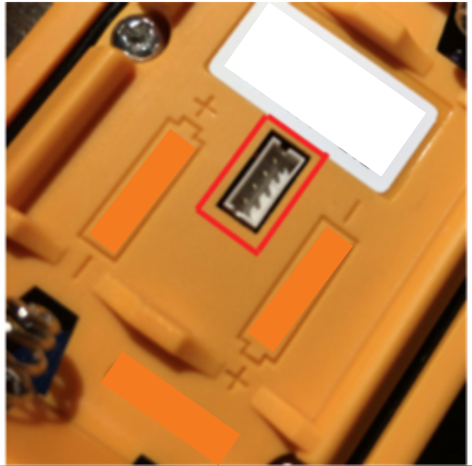


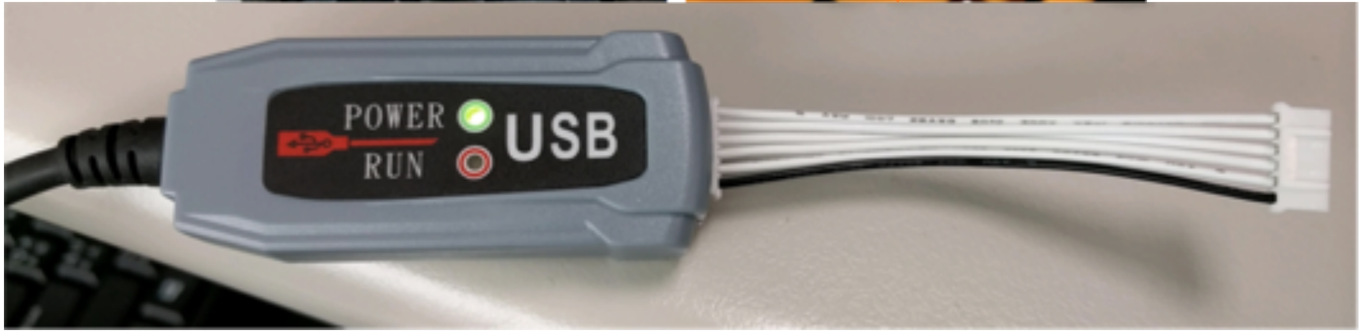
Short-range attackers

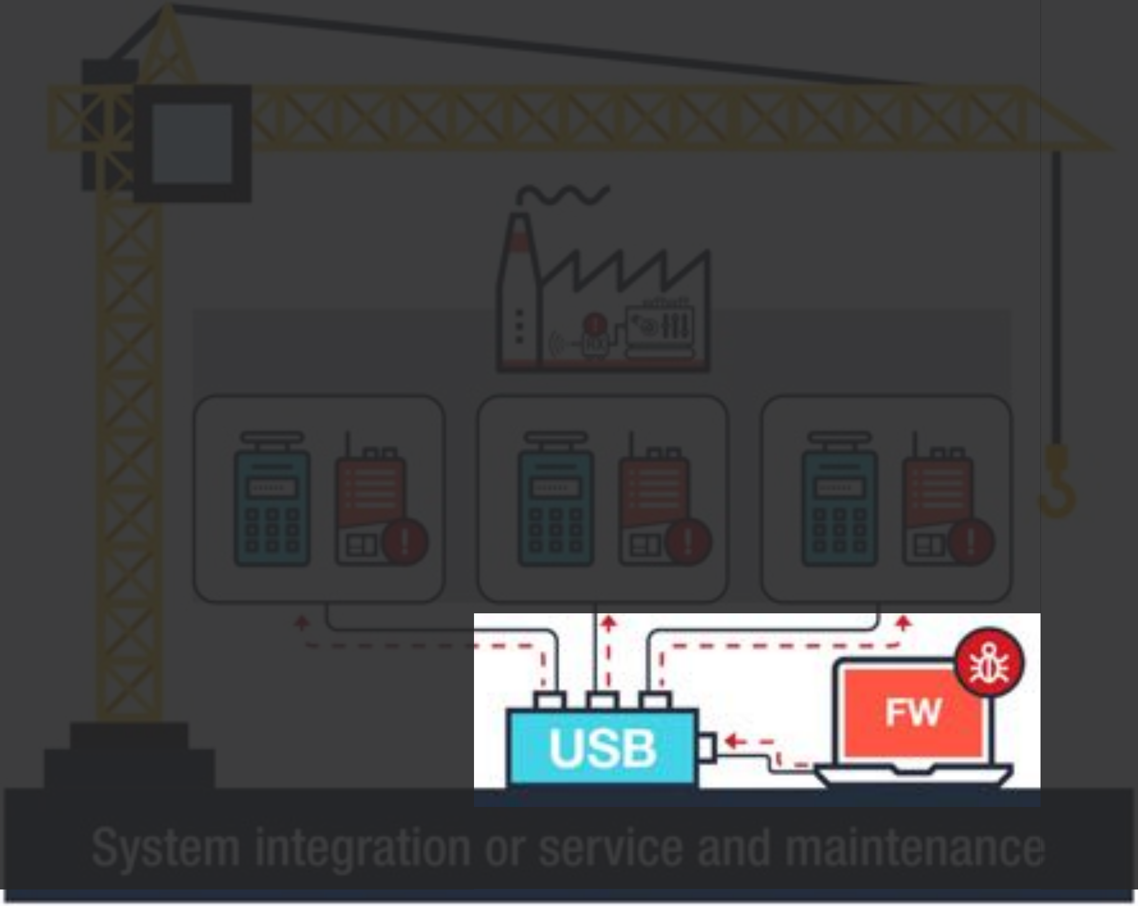
vs

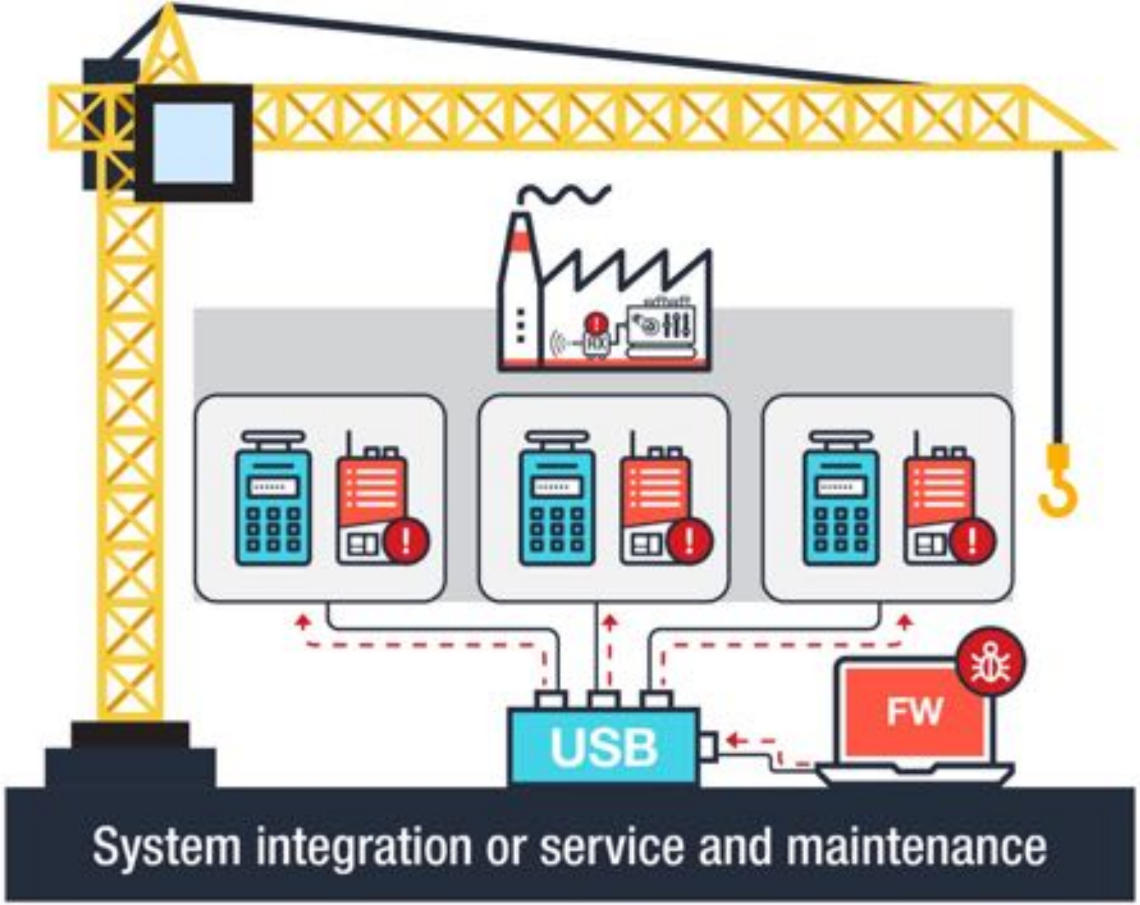
2 Internet attackers

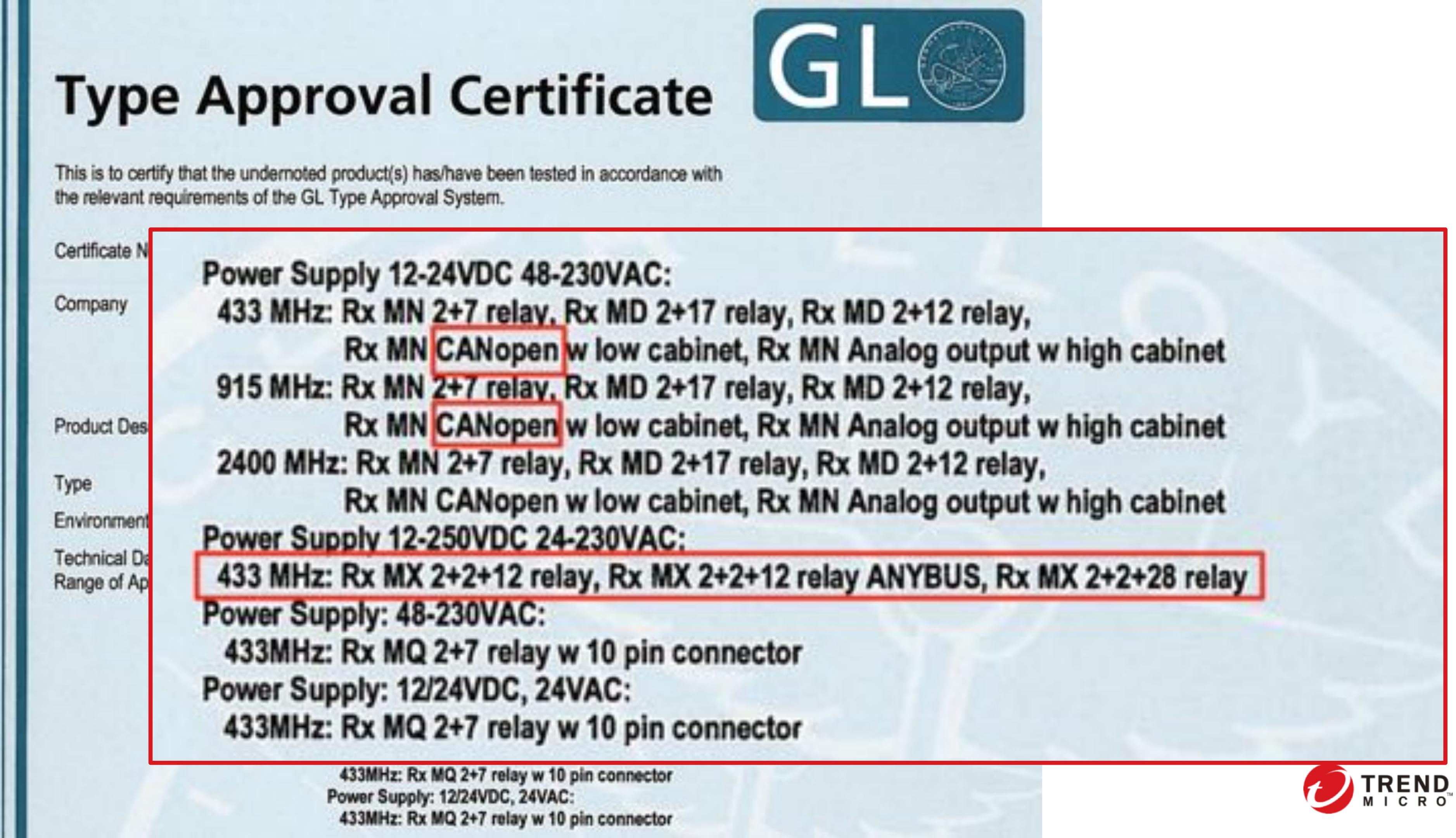

SIZE AA 1.5V
R6 UM3
SIZE AA 1.5V
R6 UM3




POWER
RUN
USB


USB
FW
System integration or service and maintenance


RX
FW
USB
System integration or service and maintenance



Type Approval Certificate

GL

This is to certify that the undernoted product(s) has/have been tested in accordance with the relevant requirements of the GL Type Approval System.

Certificate N

Company

Product Des

Type

Environment

Technical Da
Range of Ap

Power Supply 12-24VDC 48-230VAC:

433 MHz: Rx MN 2+7 relay, Rx MD 2+17 relay, Rx MD 2+12 relay,
Rx MN CANopen w low cabinet, Rx MN Analog output w high cabinet

915 MHz: Rx MN 2+7 relay, Rx MD 2+17 relay, Rx MD 2+12 relay,
Rx MN CANopen w low cabinet, Rx MN Analog output w high cabinet

2400 MHz: Rx MN 2+7 relay, Rx MD 2+17 relay, Rx MD 2+12 relay,
Rx MN CANopen w low cabinet, Rx MN Analog output w high cabinet

Power Supply 12-250VDC 24-230VAC:

433 MHz: Rx MX 2+2+12 relay, Rx MX 2+2+12 relay ANYBUS, Rx MX 2+2+28 relay

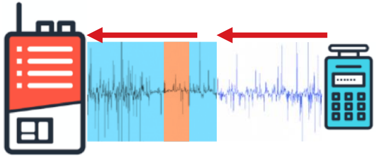
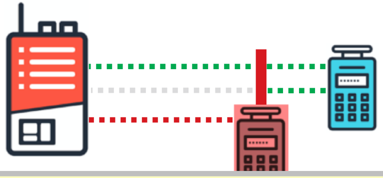
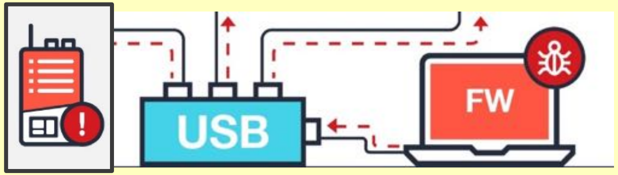
Power Supply: 48-230VAC:

433MHz: Rx MQ 2+7 relay w 10 pin connector

Power Supply: 12/24VDC, 24VAC:

433MHz: Rx MQ 2+7 relay w 10 pin connector

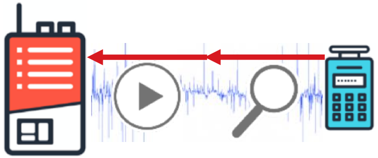
433MHz: Rx MQ 2+7 relay w 10 pin connector
Power Supply: 12/24VDC, 24VAC:
433MHz: Rx MQ 2+7 relay w 10 pin connector

ATTACK CLASS		Vendors	Difficulty	Resources
1: Replay Attack		All tested	🟥⬜⬜	$$$$
2: Command Injection		All tested	🟧🟧⬜	$$$$
3: E-Stop Abuse	E-STOP E-STOP E-STOP OFF	All tested	🟥⬜⬜	$$$$
4: Malicious Re-pairing		Some of tested	🟧🟧⬜	$$$$
5: Malicious Re-programming		All tested	🟩🟩🟩	$$$$

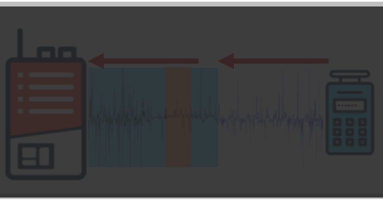
Vulnerability Patterns and Patching

ATTACK CLASS

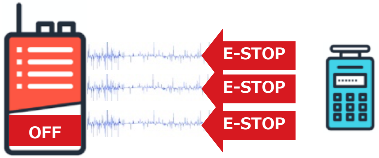
1: Replay Attack



2: Command Injection



3: E-Stop Abuse



4: Malicious Re-pairing

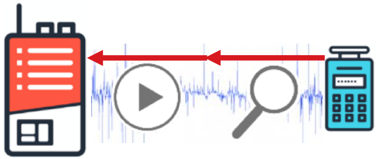
5: Malicious Re-programming

VULNERABILITY PATTERN

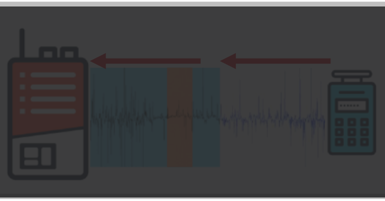
No rolling-code mechanism

ATTACK CLASS

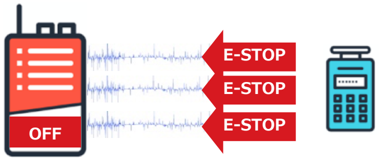
1: Replay Attack



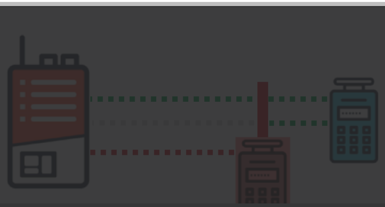
2: Command Injection



3: E-Stop Abuse



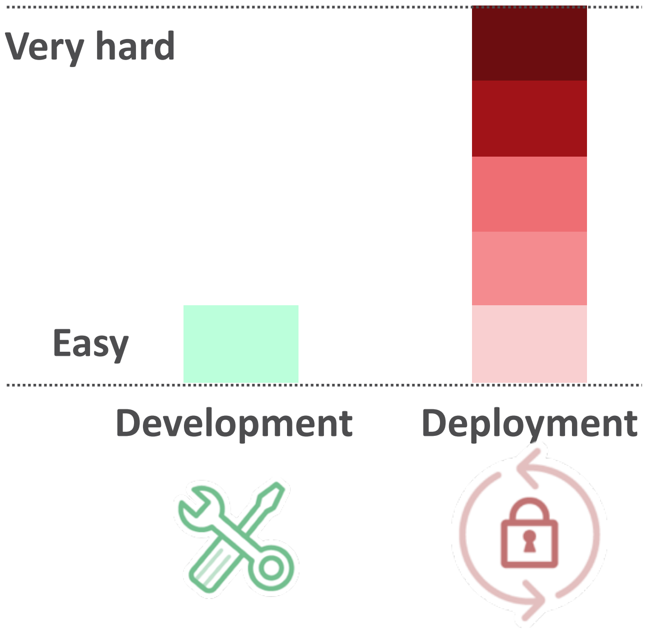
4: Malicious Re-pairing



5: Malicious Re-programming

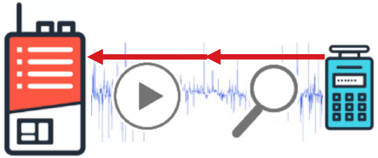
VULNERABILITY PATTERN

No rolling-code mechanism

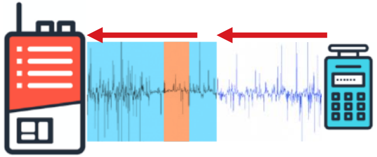


ATTACK CLASS

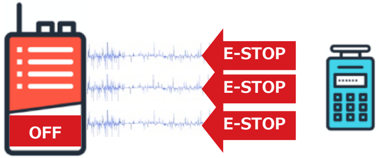
1: Replay Attack



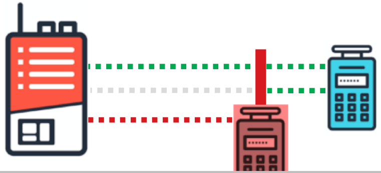
2: Command Injection



3: E-Stop Abuse



4: Malicious Re-pairing



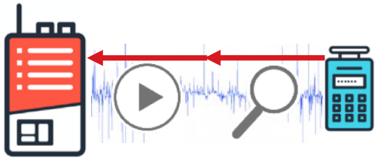
5: Malicious Re-programming

VULNERABILITY PATTERN

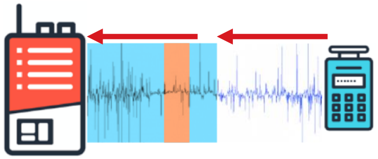
Weak or no cryptography

ATTACK CLASS

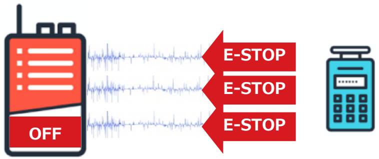
1: Replay Attack



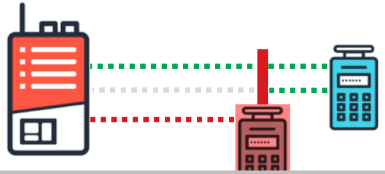
2: Command Injection



3: E-Stop Abuse



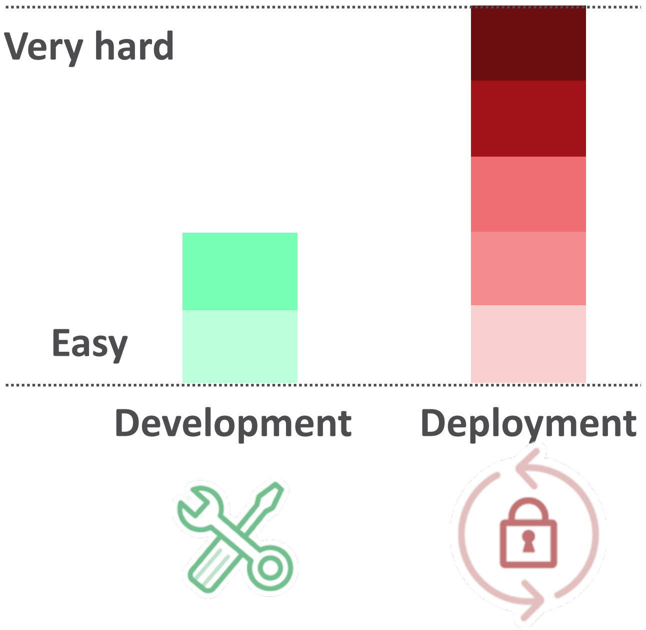
4: Malicious Re-pairing



5: Malicious Re-programming

VULNERABILITY PATTERN

Weak or no cryptography

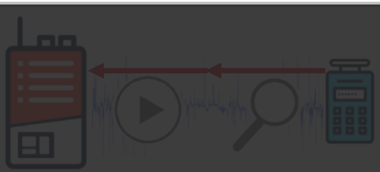


ATTACK CLASS

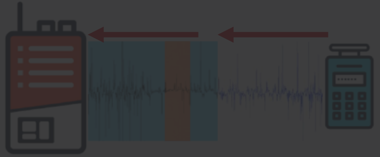
VULNERABILITY PATTERN

Lack of software protection

1: Replay Attack



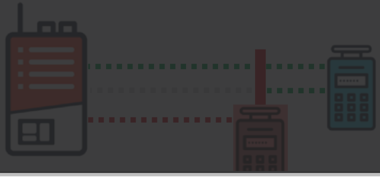
2: Command Injection



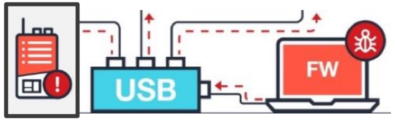
3: E-Stop Abuse

E-STOP
E-STOP
E-STOP
OFF

4: Malicious Re-pairing

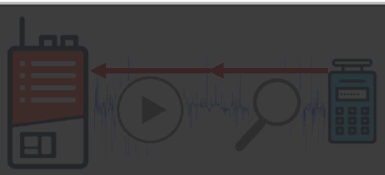


5: Malicious Re-programming

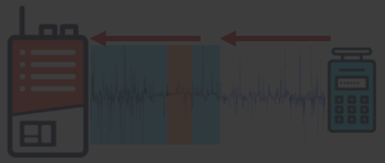


ATTACK CLASS

1: Replay Attack



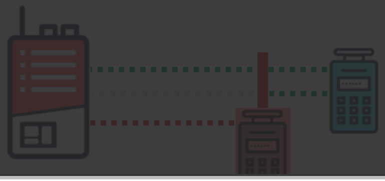
2: Command Injection



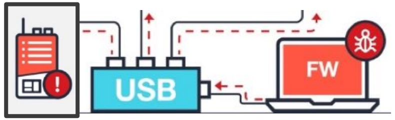
3: E-Stop Abuse

E-STOP
E-STOP
E-STOP
OFF

4: Malicious Re-pairing

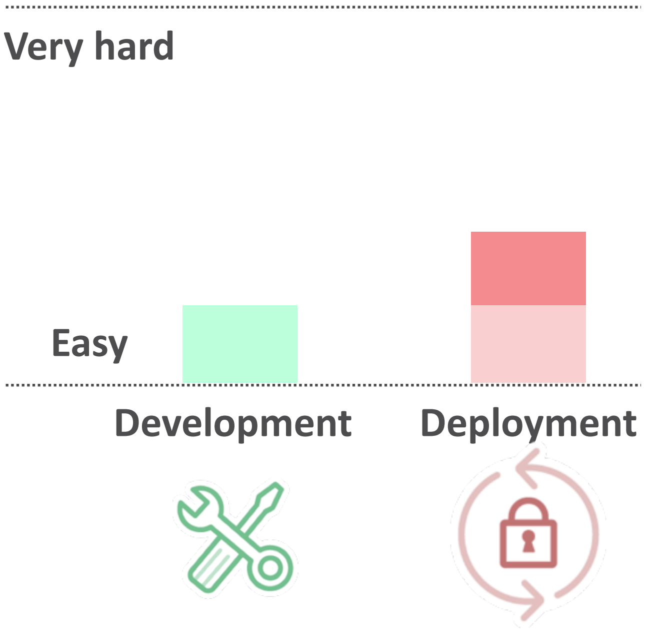


5: Malicious Re-programming

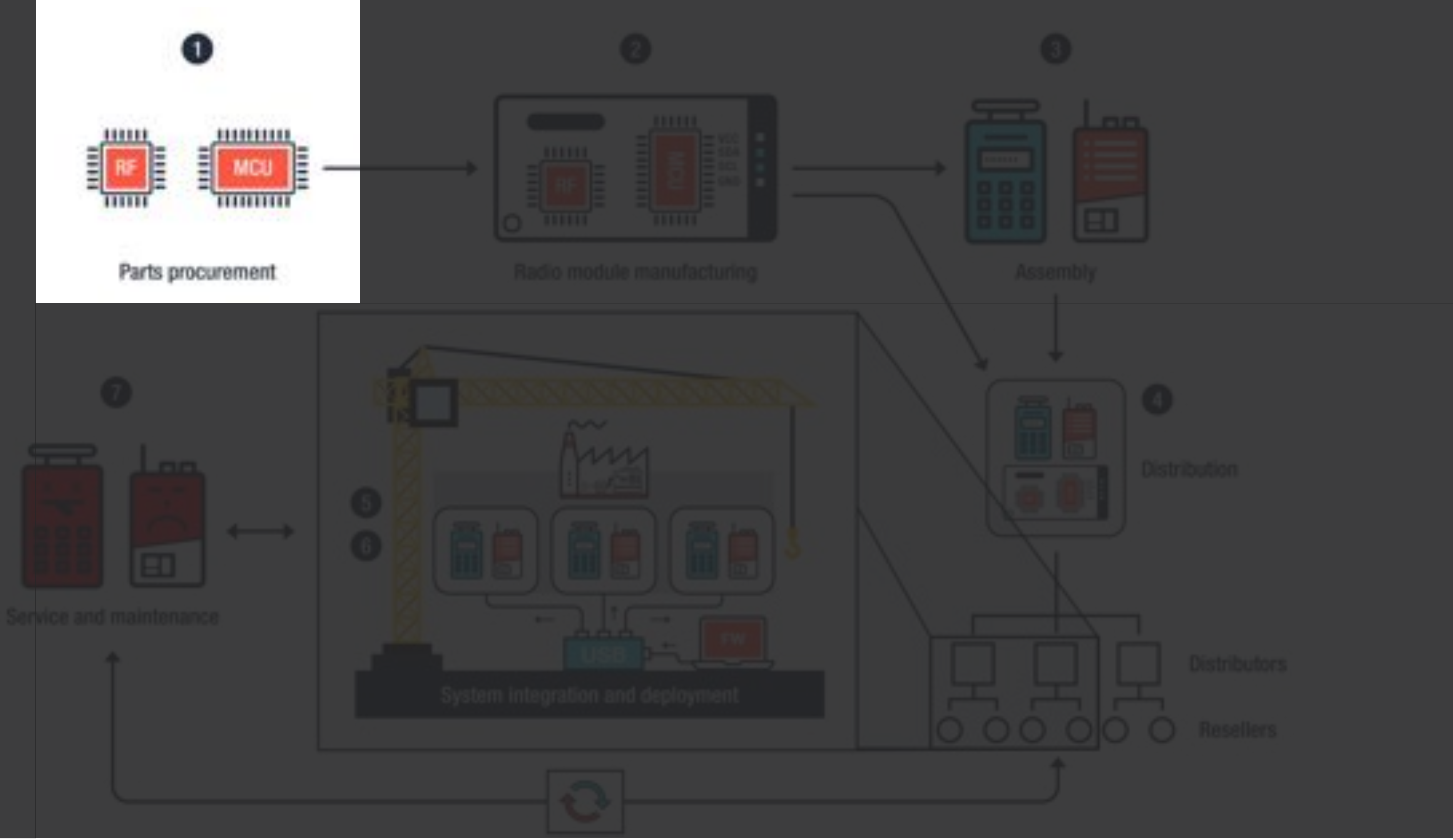


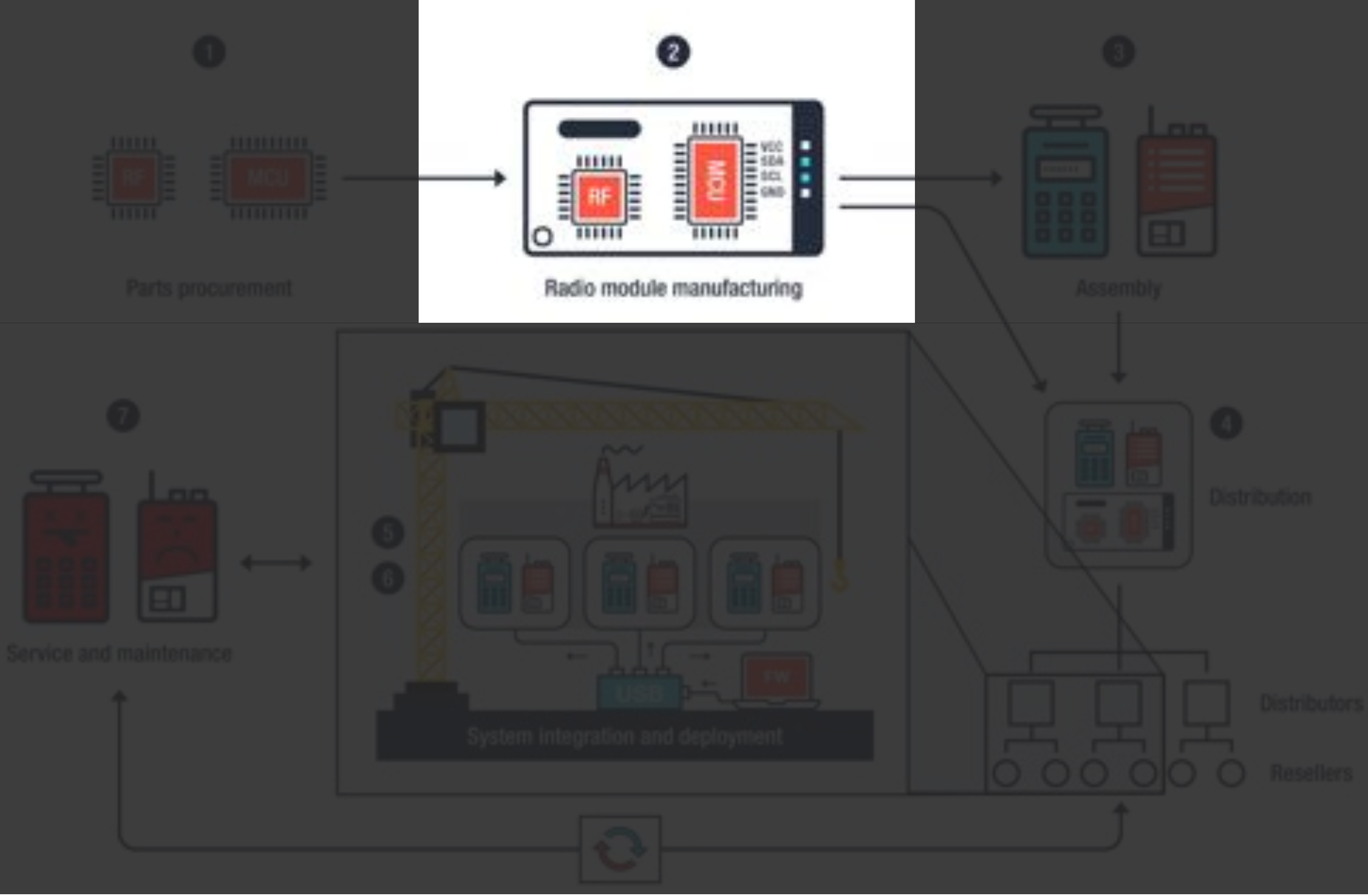
VULNERABILITY PATTERN

Lack of software protection

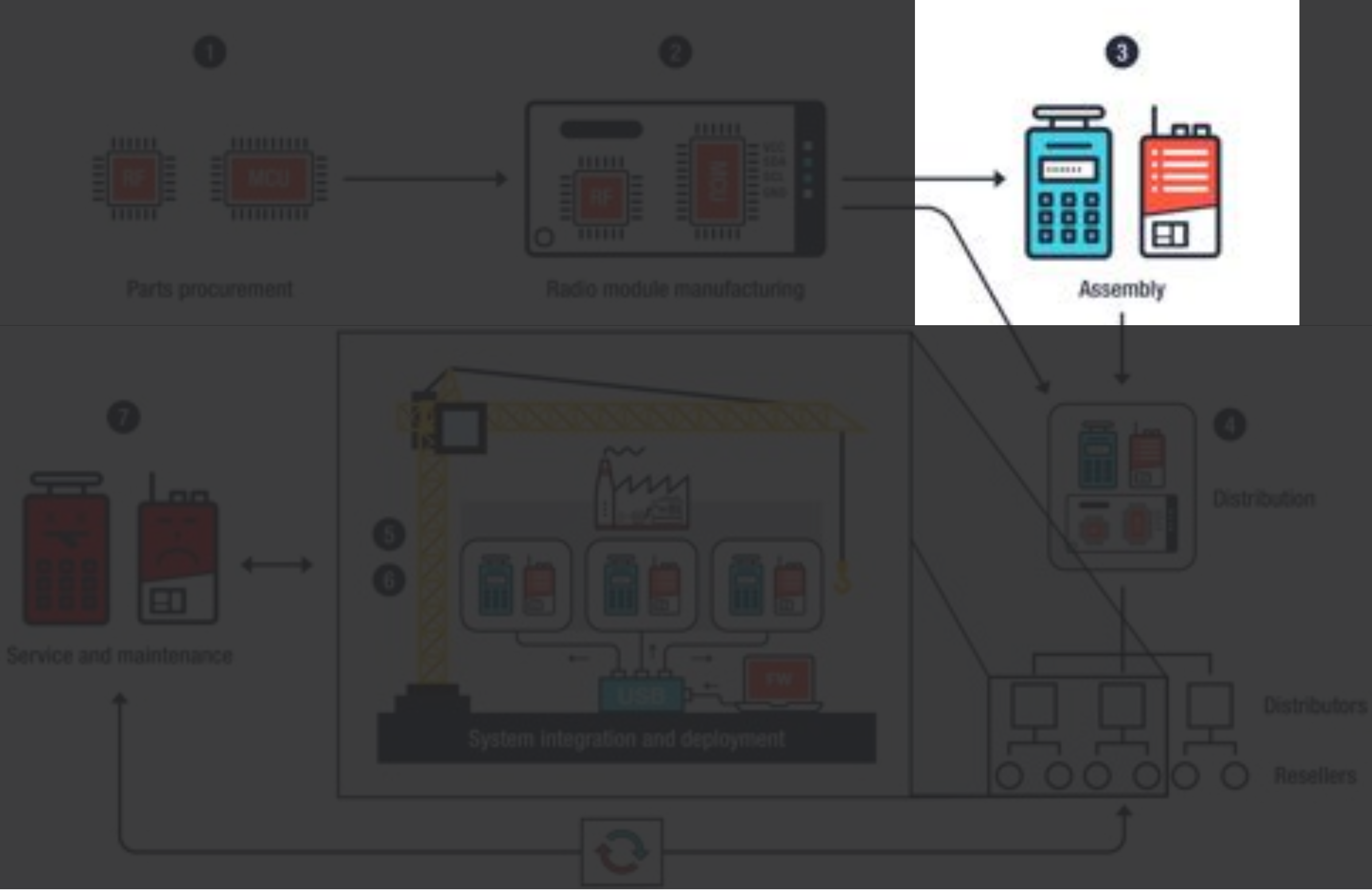


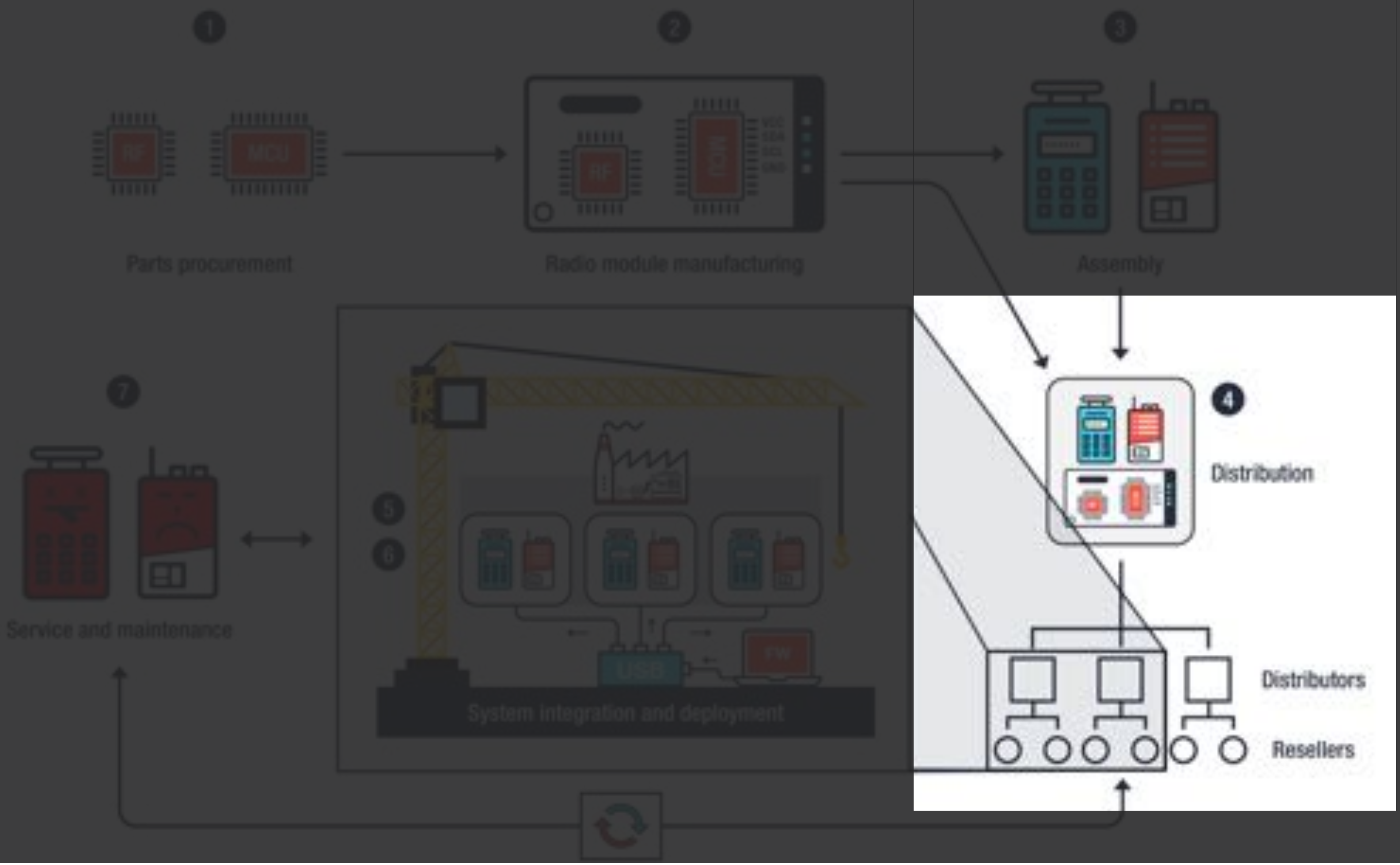
Supply Chain and Countermeasures

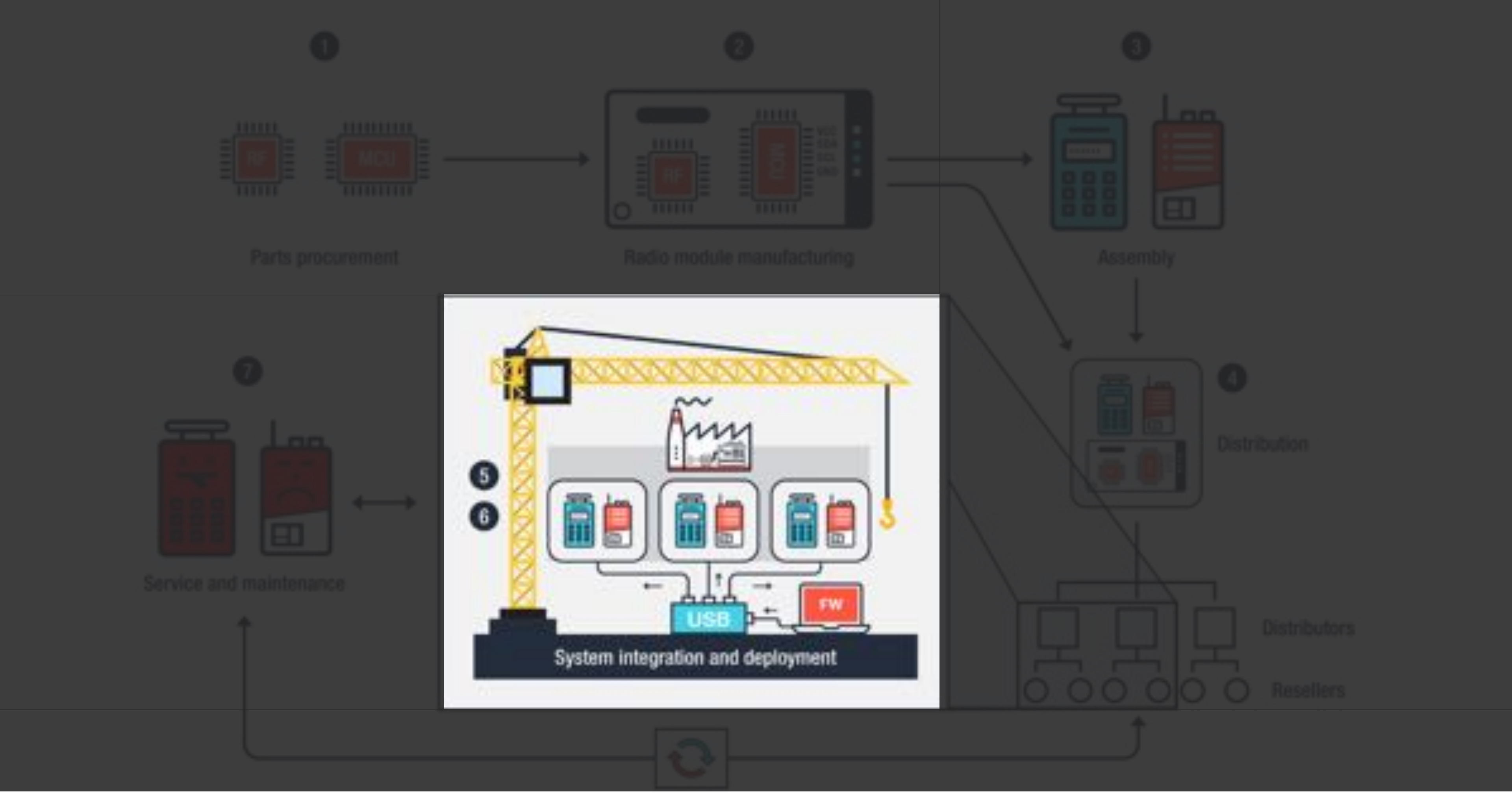

1
RF
MCU
Parts procurement
2
RF
MCU
VCC
SDA
SCL
GND
Radio module manufacturing
3
Assembly
4
Distribution
Distributors
Resellers
5
6
USB
FW
System integration and deployment
7
Service and maintenance

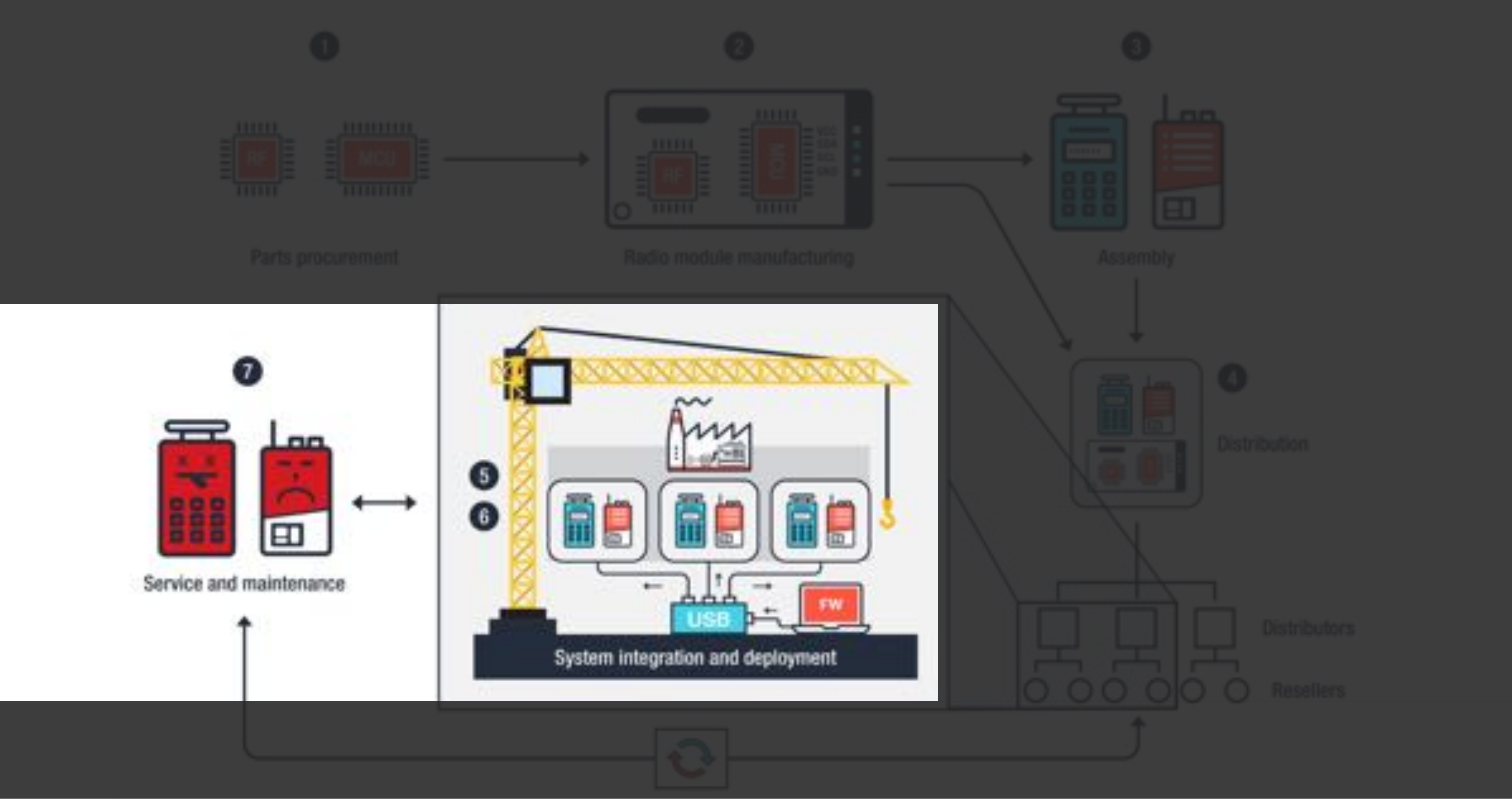


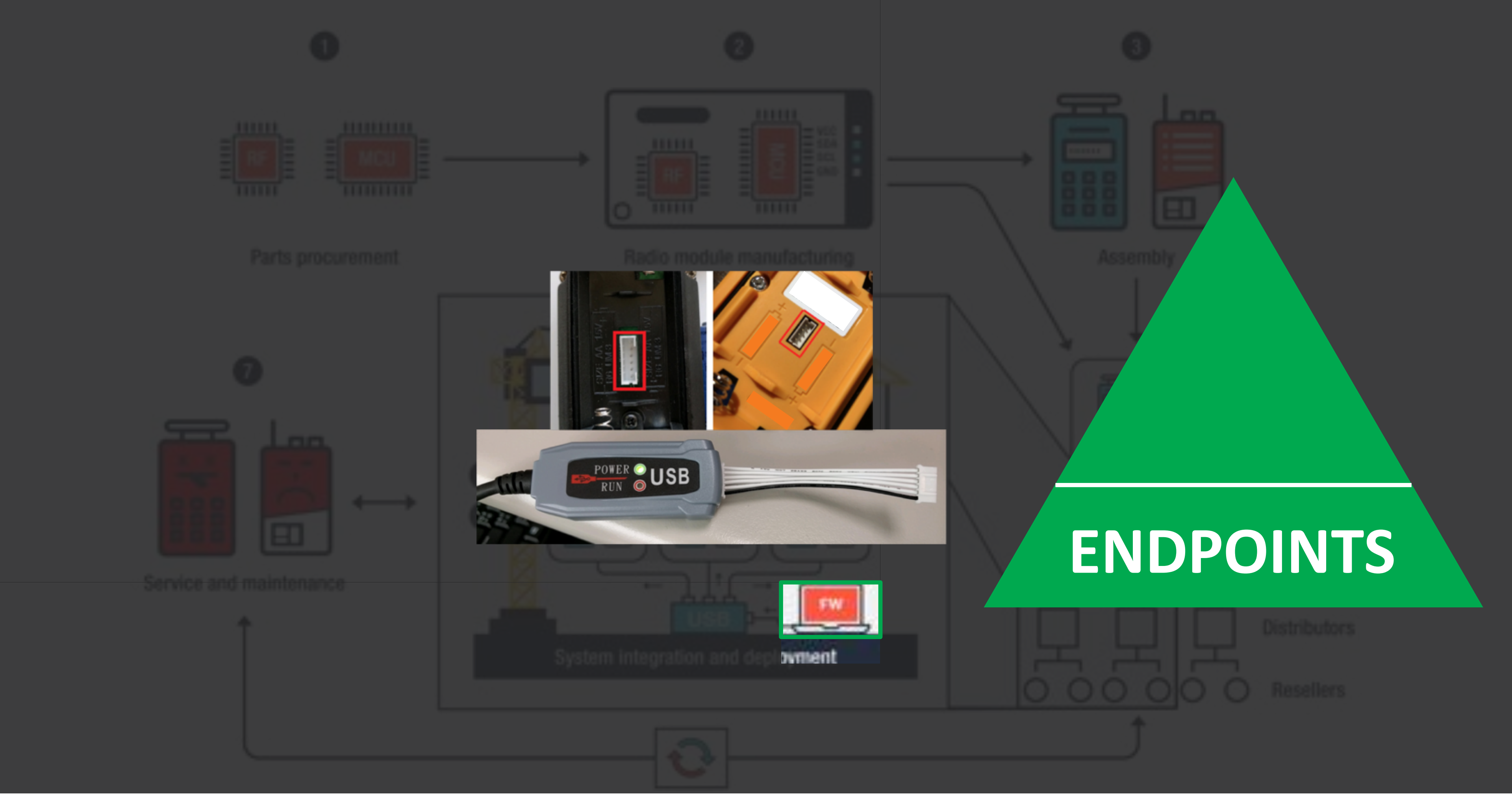
1
RF
MCU
Parts procurement
2
RF
MCU
VCC
SDA
SCL
GND
Radio module manufacturing
3
Assembly
4
Distribution
Distributors
Resellers
5
6
System integration and deployment
USB
FW
7
Service and maintenance


1
RF
MCU
Parts procurement
2
RF
MCU
VCC
SDA
SCL
GND
Radio module manufacturing
3
Assembly
4
Distribution
Distributors
Resellers
7
Service and maintenance
5
6
USB
FW
System integration and deployment

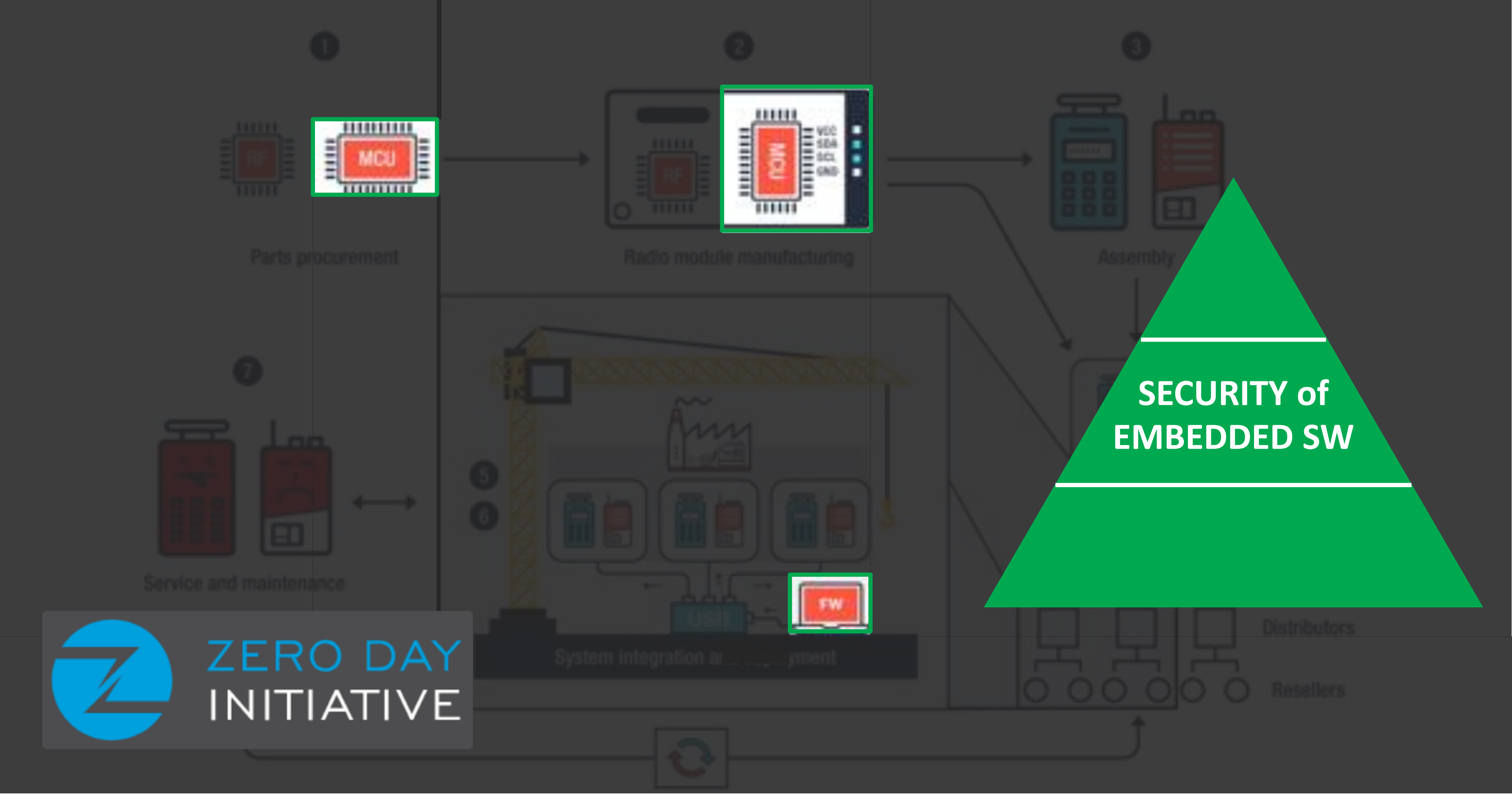

1
RF
MCU
Parts procurement
2
RF
ROM
VCC
SDA
SCL
GND
Radio module manufacturing
3
Assembly
4
Distribution
Distributors
Resellers
7
Service and maintenance
5
6
USB
FW
System integration and deployment


1
RF
MCU
Parts procurement
2
RF
MCU
VCC
SDA
SCL
GND
Radio module manufacturing
3
Assembly
4
Distribution
Distributors
Resellers
5
6
USB
FW
System integration and deployment
7
Service and maintenance


1
2
3
RF
MCU
Parts procurement
Radio module manufacturing
Assembly
4
Distribution
5
6
7
Service and maintenance
USB
FW
System integration and deployment
Distributors
Resellers

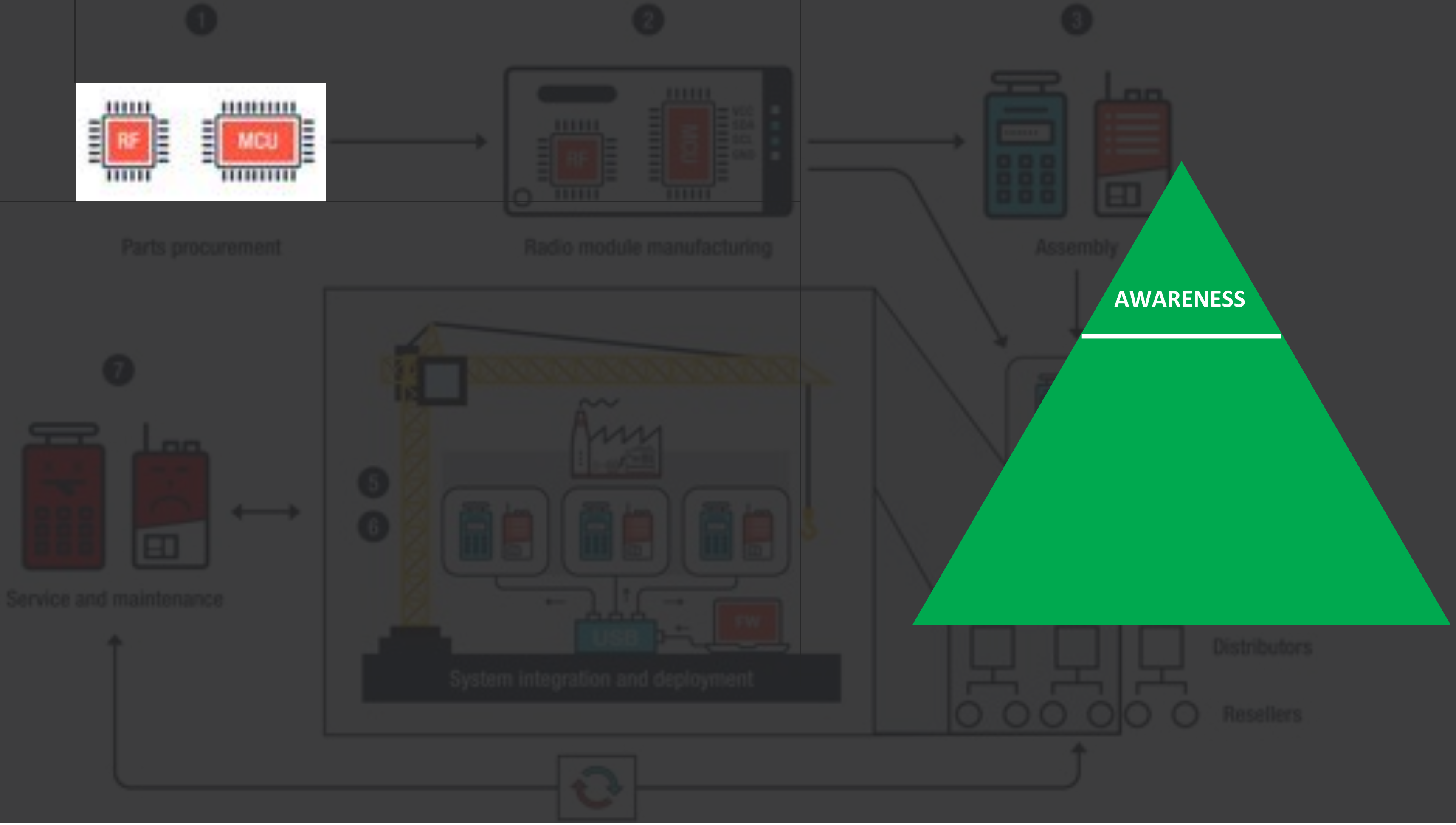

1
RF
MCU
Parts procurement
2
RF
MCU
VCC
SDA
SCL
GND
Radio module manufacturing
3
Assembly
7
Service and maintenance
POWER
RUN
USB
FW
USB
System integration and deployment
Distributors
Resellers

ENDPOINTS

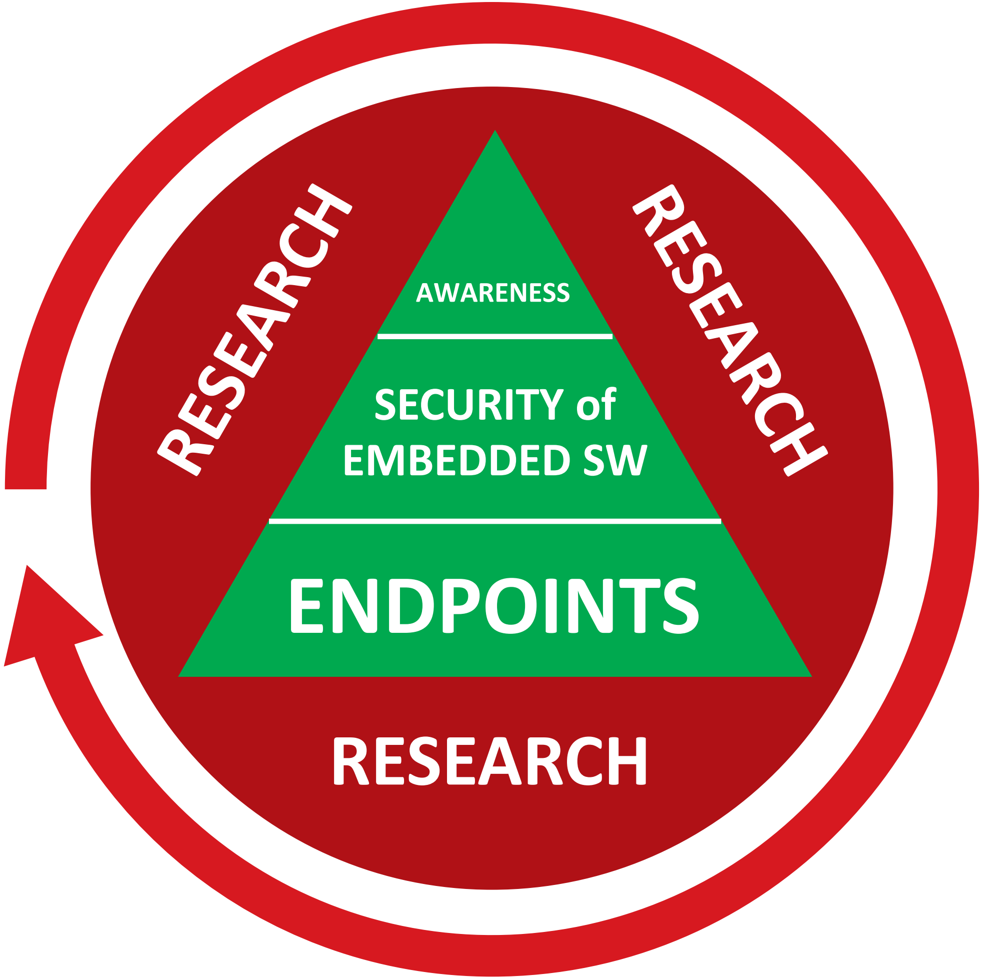


SECURITY of EMBEDDED SW

ZERO DAY INITIATIVE


1
2
3
RF
MCU
RF
MCU
VCC
SDA
SCL
GND
Parts procurement
Radio module manufacturing
Assembly
7
5
6
Service and maintenance
USB
FW
System integration and deployment
Distributors
Resellers

AWARENESS


RESEARCH

RESEARCH

AWARENESS

SECURITY of EMBEDDED SW

ENDPOINTS

RESEARCH

セッションID：E-1

IT Risks and Threats on Safety of Operational Technology

A Case Study on Wireless Remote Controllers from the Eyes of the Attackers

トレンドマイクロ株式会社
Trend Micro Research

Federico Maggi, PhD / @phretor
Senior Threat Researcher

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro InterScan WebManager SCC、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Securing Your Journey to the Cloud、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDIオプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポート プレミアム、Airサポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、およびTrend Micro Policy-based Security Orchestrationは、トレンドマイクロ株式会社の登録商標です。本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。