RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART3-T09**

IOT: Fix the Bugs That Leave Customers Inconvenienced, Stranded, or Dead

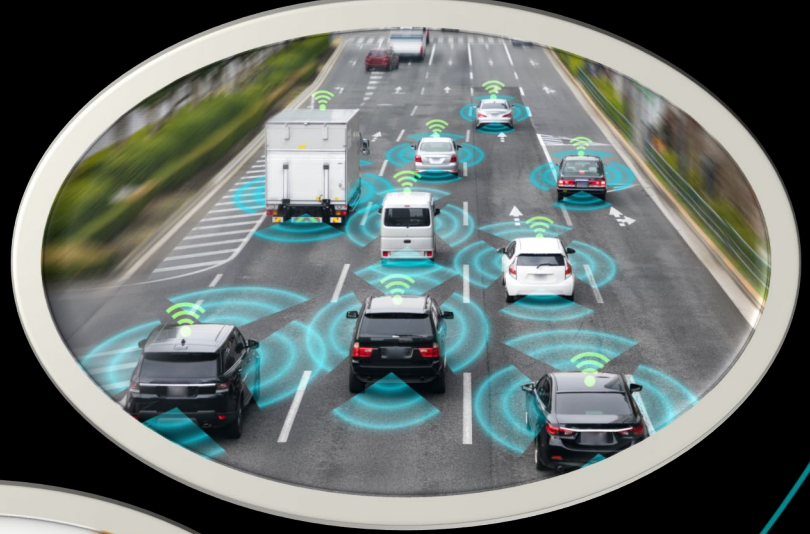
Scott W Register

VP Security Solutions
Keysight
@swregister

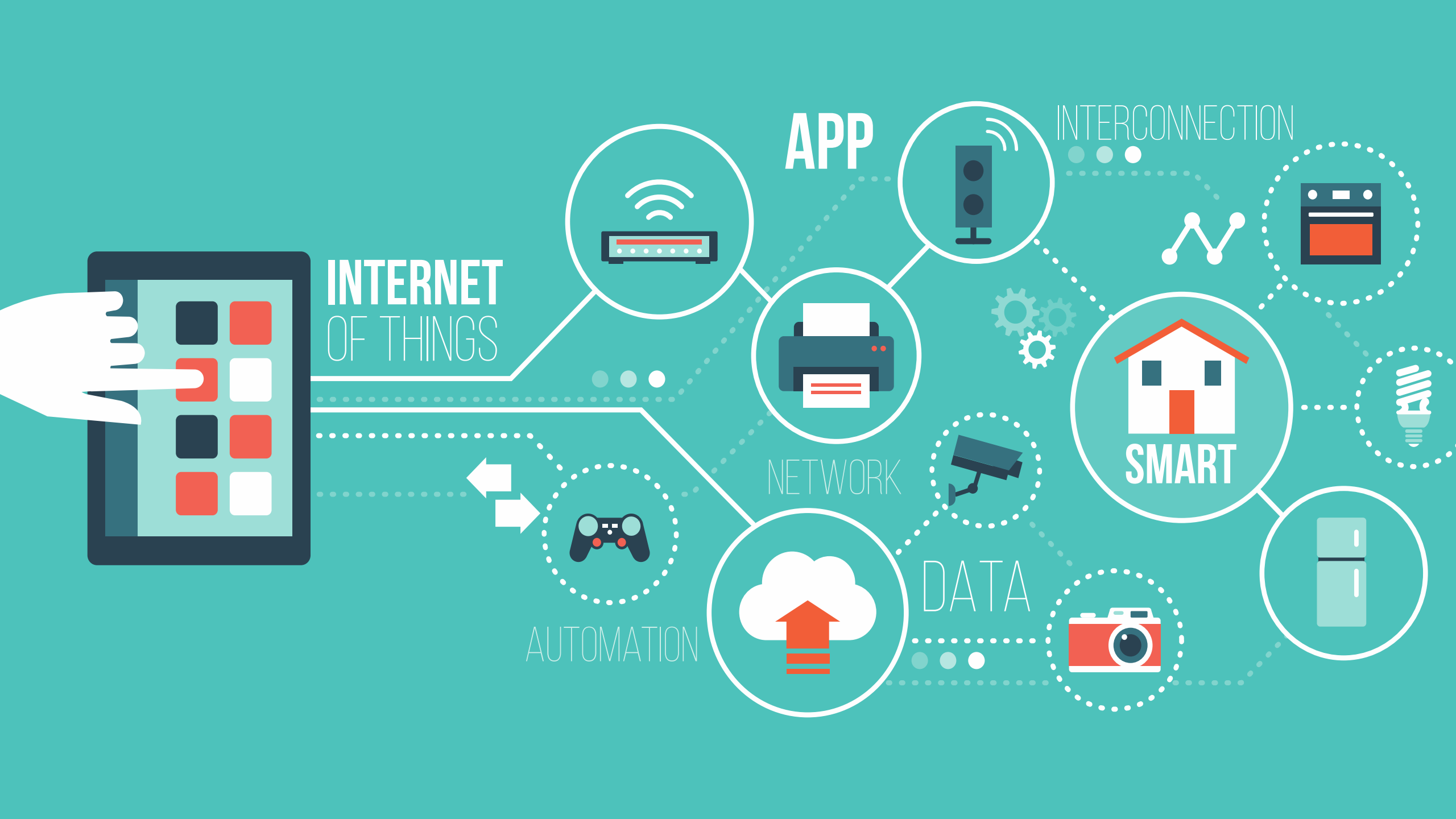
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.




SICKNESS RATE

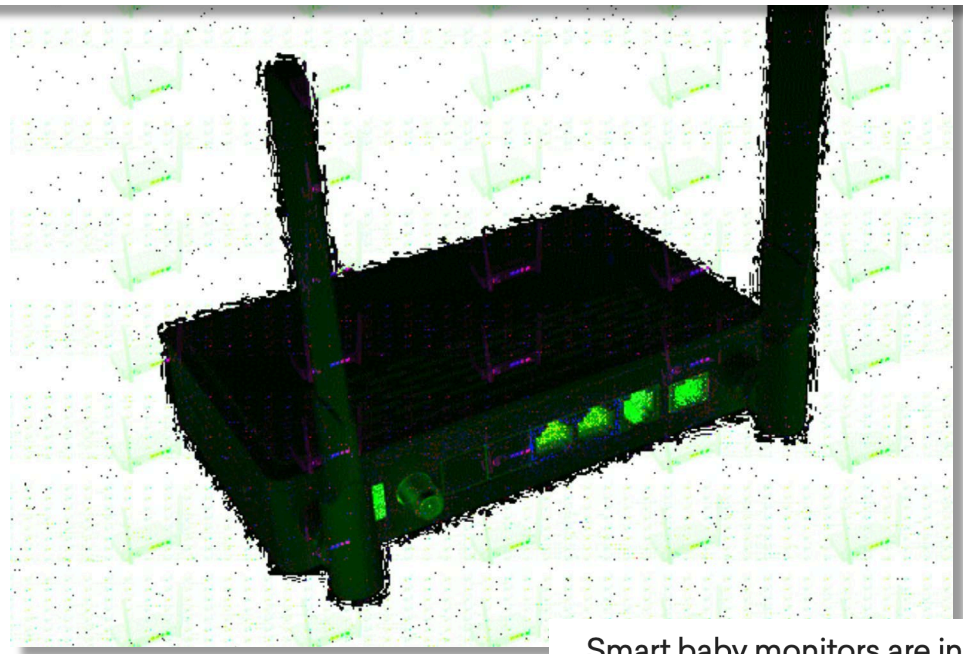

INTERNET
OF THINGS
APP
INTERCONNECTION
NETWORK
SMART
AUTOMATION
DATA

IOT Devices Are Plagued With Vulnerabilities

ANTI-MALWARE RESEARCH • IOT RESEARCH • WHITEPAPERS • 1 min read •

Ring Video Doorbell Pro Under the Scope

Hundreds of thousands of Realtek-based devices under attack from IoT botnet



Smart baby monitors are increasingly popular targets for hackers

B.Braun Infusomat Pumps Could Let Attackers Remotely Alter Medication Dosages

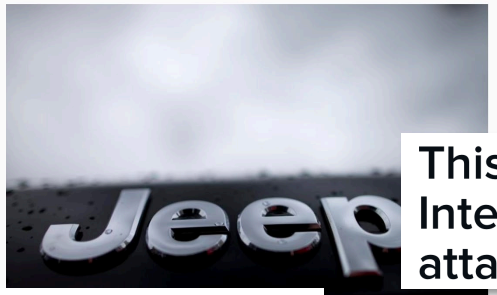
August 25, 2021 Ravie Lakshmanan

How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

This article is more than 5 years old.



herokee has some

MYCAR

A Remote-Start App Exposed Thousands of Cars to Hackers

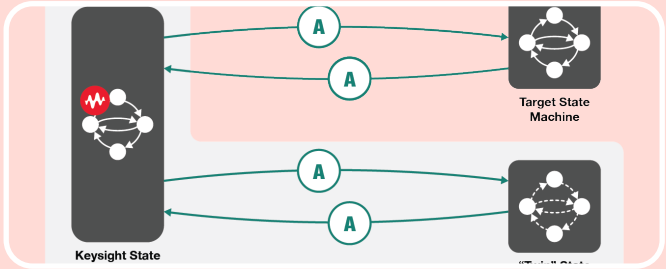
ANDY GREENBERG

This old security vulnerability left millions of Internet of Things devices vulnerable to attacks

Aspects of IOT for Cybersecurity Validation

Vulnerability Assessment

- Weak/Default Passwords
- Deprecated encryption
- Invalid certs
- APK packages
- ADB interface
- Exposed services
- Old/unpatched OS



Protocol Fuzzing

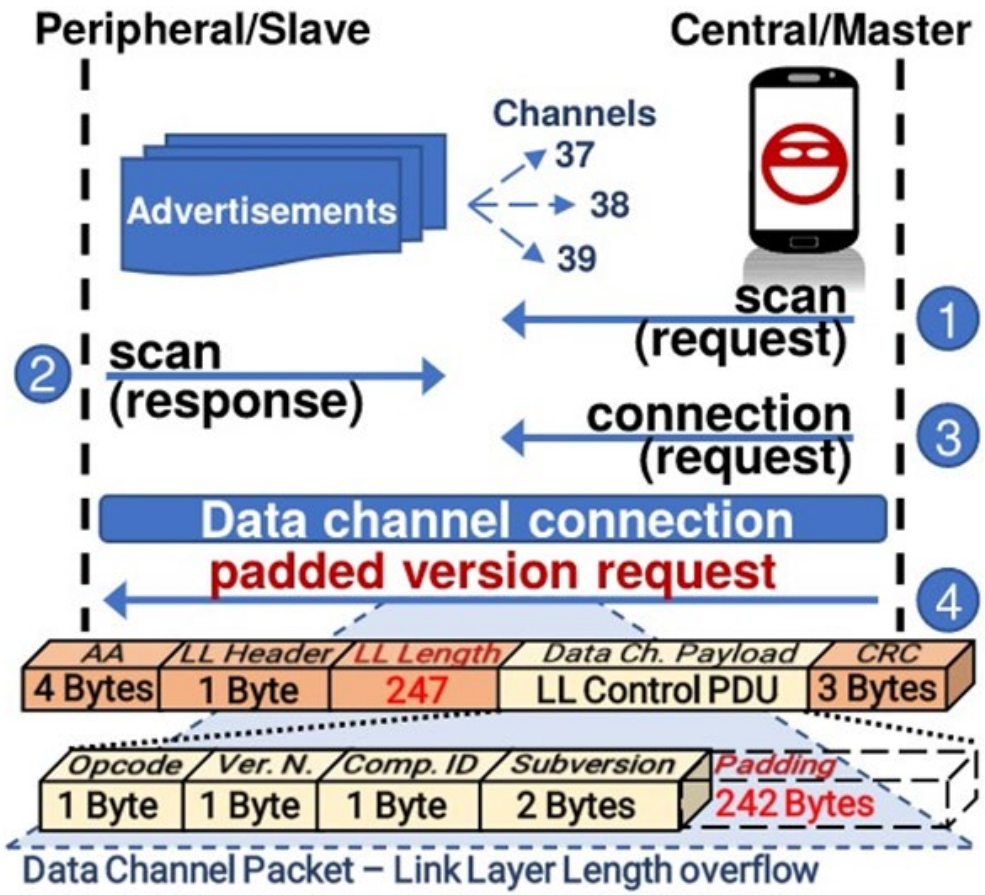
- Weaknesses in protocol stack
- Supply chain vulnerabilities from SOC
- Trigger crash / reboot / security bypass
- Can be difficult to find
- Harder to fix post-deployment

Cloud Services

- MFA protection
- Certificate and validation
- Access logging
- IAM

Protocol Fuzzing

- Systematic injection of errors into protocol stream
- Especially effective during handshake
- Malformed, repeated, out-of-order packets
- Finds flaws embedded in communication chipsets

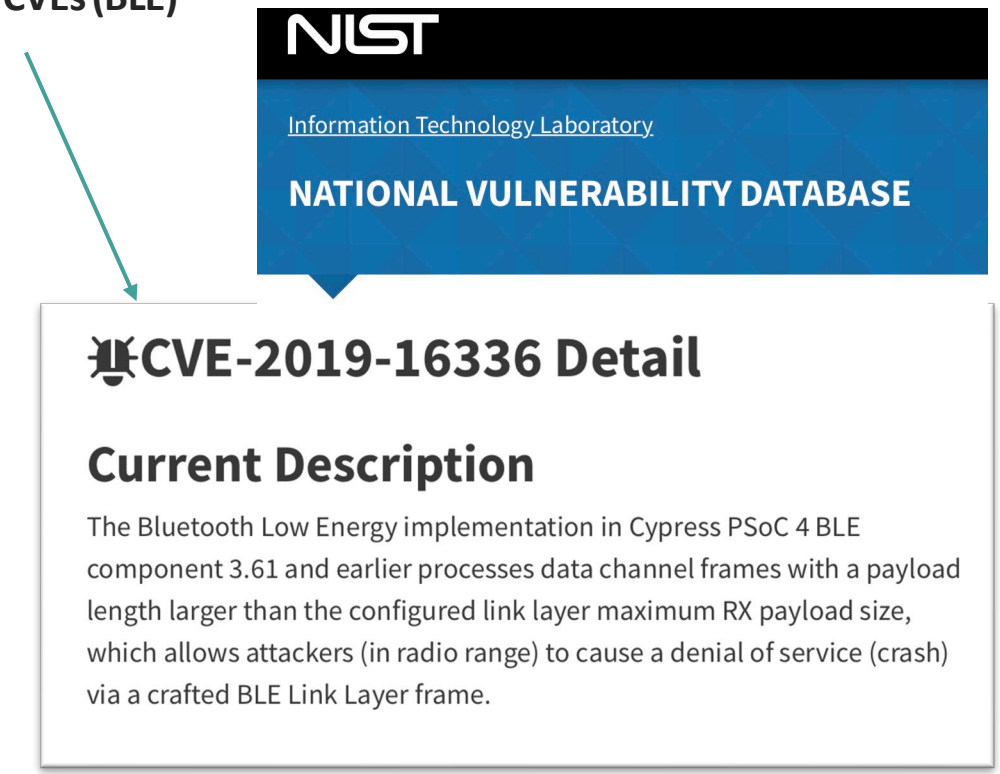


Vulnerability Assessment

- Scanning a device for weaknesses to specific attacks
- Library of known attacks is constantly evolving
- Typically directed at operating system and applications
- Also includes guessable passwords, weak encryption, and certificate errors

Link Layer related CVEs (BLE)

- CVE-2019-16336
- CVE-2019-17519
- CVE-2019-17517
- CVE-2019-17518
- CVE-2019-17061
- CVE-2019-17060
- CVE-2019-19193



Source: NIST

Vulns Discovered in Post-Market Devices

← Home / Medical Devices / Medical Device Safety / Safety Communications

- SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication
- Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers: Safety Communication
- URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication
- Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication
- Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

Share | Tweet | Linkedin | Email | Print

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. Software to exploit these vulnerabilities in certain situations is already publicly available.

Security researchers have identified 12 vulnerabilities, named "SweynTooth," associated with a wireless communication technology known as Bluetooth Low Energy (BLE). BLE allows two devices to "pair" and exchange information to perform their intended functions while preserving battery life.

The potential impacts of the SweynTooth vulnerabilities fall into three categories. An unauthorized user can wirelessly exploit these vulnerabilities to:

- **Crash** the device. The device may stop communicating or stop working.
- **Deadlock** the device. The device may freeze and stop working correctly.
- **Bypass security** to access device functions normally available only to an authorized user.

The FDA is currently aware of several system-on-a-chip (SoC) manufacturers that are affected by these vulnerabilities:

- Texas Instruments
- NXP
- Cypress
- Dialog Semiconductors
- Microchip
- STMicroelectronics
- Telink Semiconductor

FDA U.S. FOOD & DRUG ADMINISTRATION

← Home / Medical Devices / Medical Device Safety / Safety Communications / SweynTooth Cybersecurity Vulnerabilities

The FDA is currently aware of several system-on-a-chip (SoC) manufacturers that are affected by these vulnerabilities:

- Texas Instruments
- NXP
- Cypress
- Dialog Semiconductors
- Microchip
- STMicroelectronics
- Telink Semiconductor

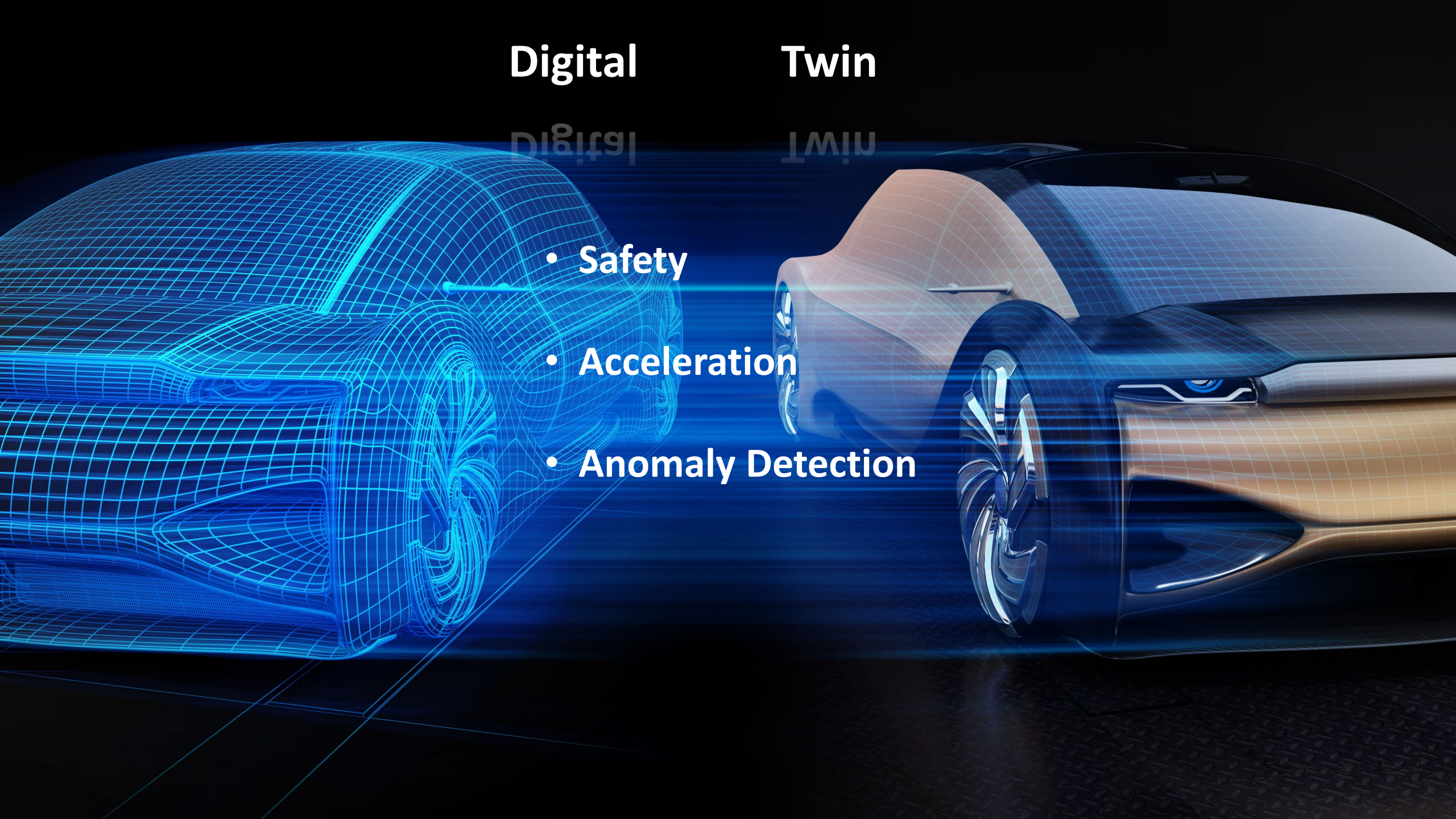
- **Crash** the device. The device may stop communicating or stop working.
- **Deadlock** the device. The device may freeze and stop working correctly.
- **Bypass security** to access device functions normally available only to an authorized user.

Source: FDA

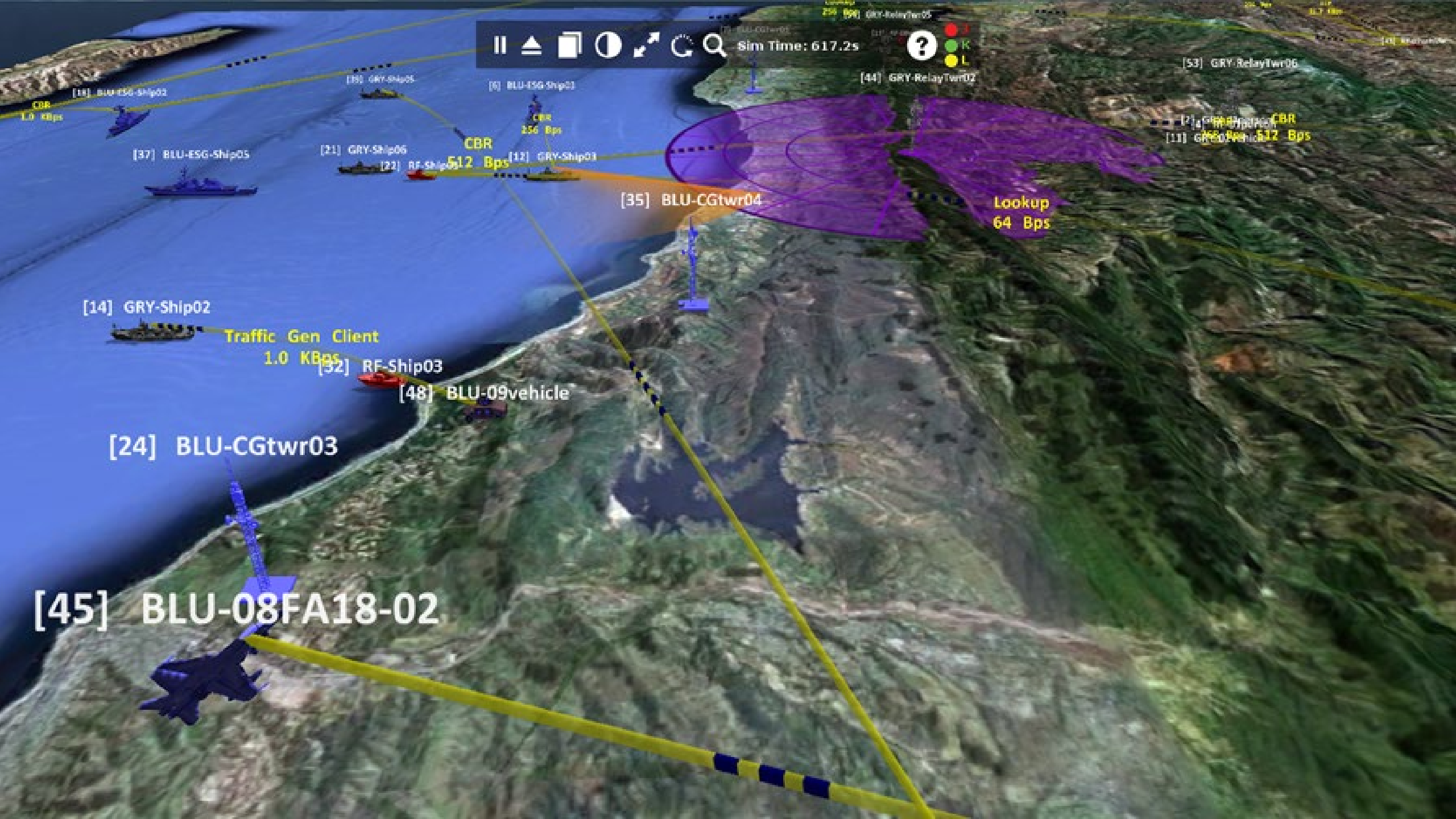
RSAConference2022

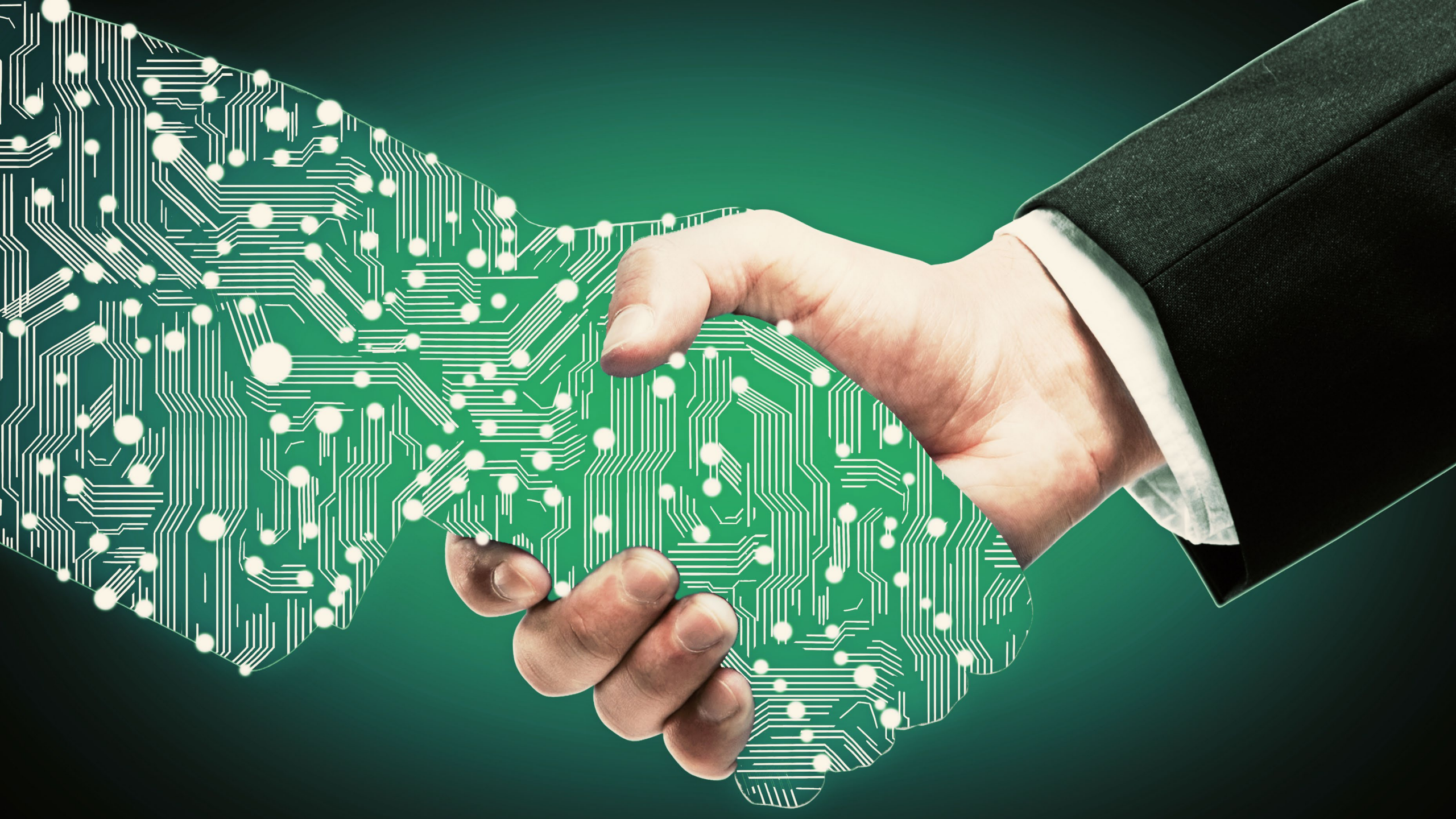
Digital Twins

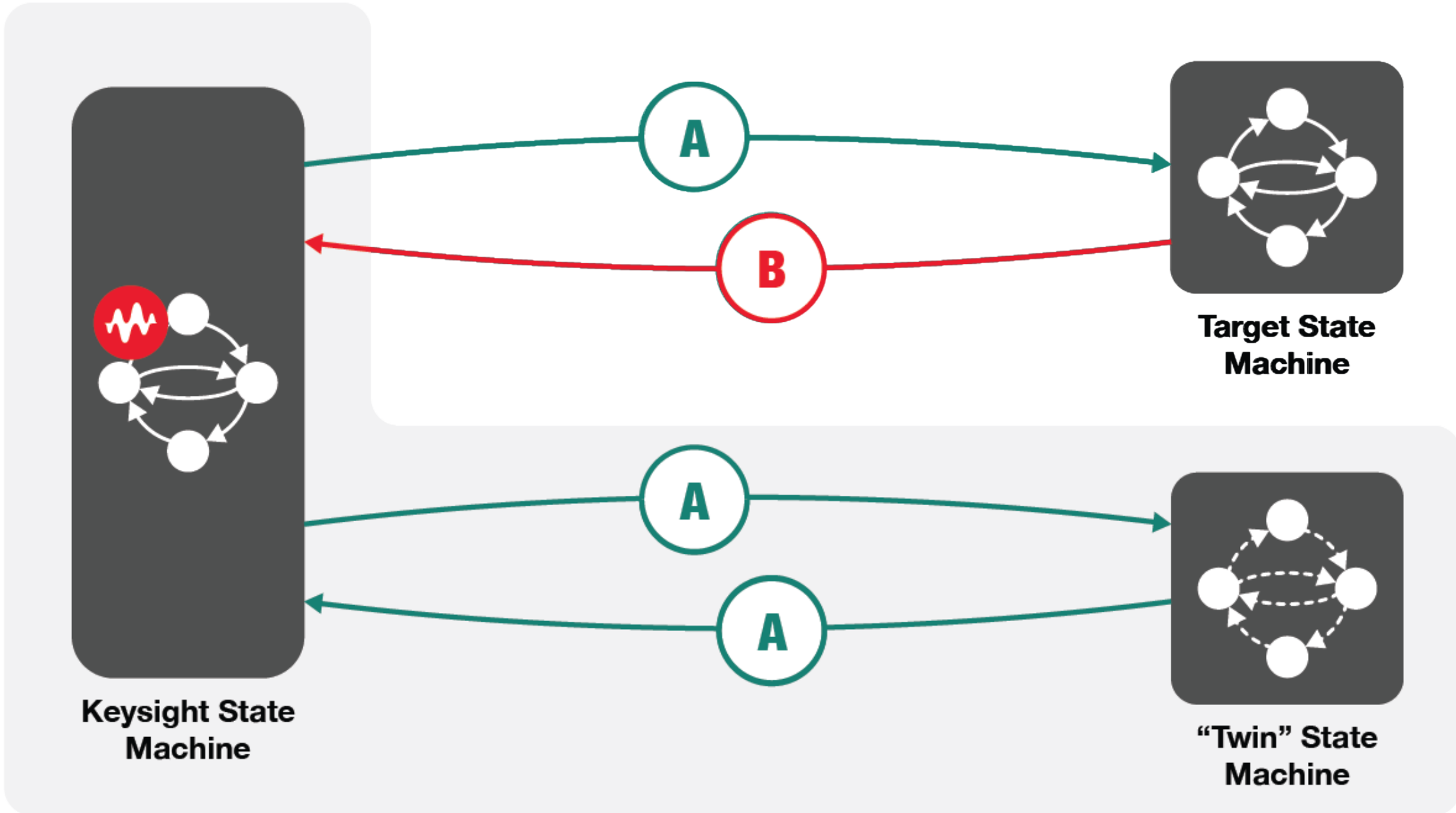
Digital Twin



- Safety
- Acceleration
- Anomaly Detection


Sim Time: 617.2s
[44] GRY-RelayTwr02
[53] GRY-RelayTwr06
[37] BLU-ESG-Ship05
[21] GRY-Ship06
[22] RF-Ship04
[6] BLU-ESG-Ship01
CBR
256 Bps
CBR
512 Bps
[12] GRY-Ship03
[35] BLU-CGtwr04
Lookup
64 Bps
[14] GRY-Ship02
Traffic Gen Client
1.0 KBps
[32] RF-Ship03
[48] BLU-09vehicle
[24] BLU-CGtwr03
[45] BLU-08FA18-02




A
B
Target State Machine
A
A
Keysight State Machine
"Twin" State Machine

If You Build Stuff:
Apply What You Have Learned Today

- Next week you should:
  - Find out if you even do cybersecurity testing – VA? Fuzzing?
- In the first three months following this presentation you should:
  - Understand the attack surface exposed by your devices
  - Map out the probability of compromise and impact of compromise
  - Understand the risks imposed by your supply chain
- Within six months you should:
  - Define a cybersecurity evaluation regimen as part of quality control

If You Deploy/Manage Stuff:
Apply What You Have Learned Today

- Next week you should:
  - Build an inventory of the connected devices, IP or otherwise, on your network
- In the first three months following this presentation you should:
  - Understand how accessible (RF? Ethernet? Routed IP?) your devices are
  - Tabletop exercise of exposure of your connected/IOT devices
- Within six months you should:
  - Have a testing mechanism in place for connected devices with higher risk profiles
  - Implement a plan for resolving your IOT supply chain issues

Q&A