

Automotive Cybersecurity Test Platform

Introduction

The fully autonomous vehicle is the dream for most of the automakers and their customers around the world. To make this happen, the car needs to be connected to the outside world. These connections, however, open the car to outside interference. Keysight can help you find vulnerabilities before anyone else does.



How to Configure Your System

In this guide, we will explain how to configure the SA8710A system to fit your needs. The Keysight SA8710A Automotive Cybersecurity test solution is a flexible solution that allows you to test the robustness of your system's security. Keysight offers a combination of hardware plus software, which when used in tandem, are designed to test the resiliency of your ECUs, systems, or full developed cars. The hardware provides the gateways to your devices via cellular, WLAN, Bluetooth, CAN and more . This hardware is complemented by Keysight PathWave-based software options which control your connectivity gateways, and the Debian Linux-based PC which contains many of the penetration toolsets used in this solution.

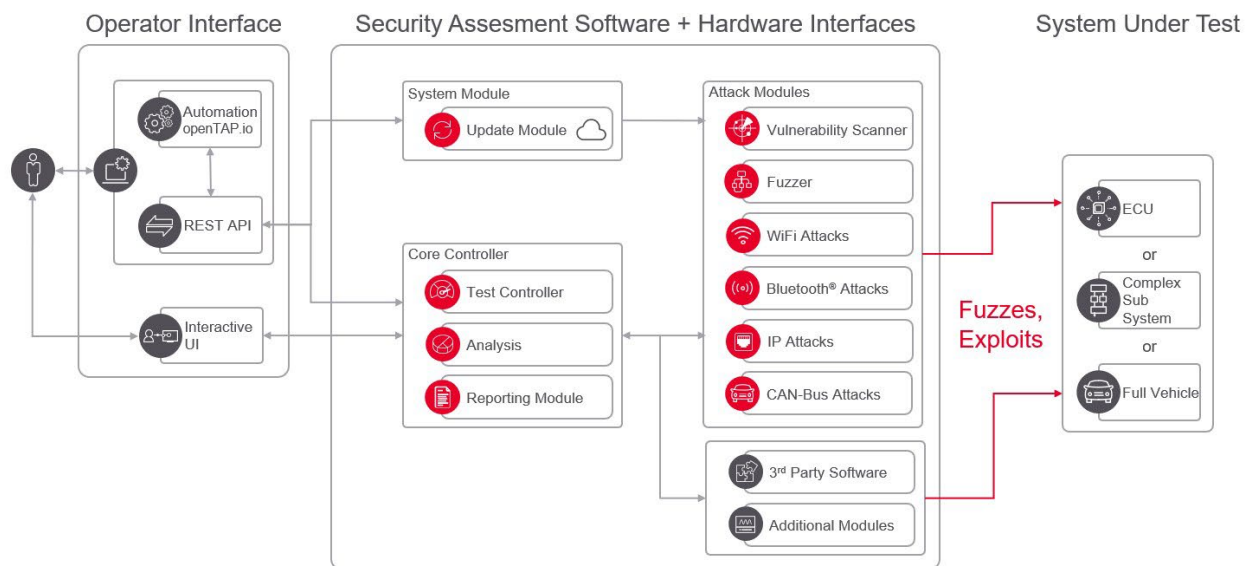


Figure 1. SA8710A high-level architecture

Keysight has made it as easy as possible to configure your SA8710A solution. All the exploitation software and automated attacks are already built into the base software, so you need to choose how you want to connect to your device(s) under test and the correct control software. Given the modular nature of the solution, it is also possible to retrofit hardware and software connectivity options after the initial purchase to meet your testing requirements as they arise. Let's start with the hardware configuration.

Hardware Configuration

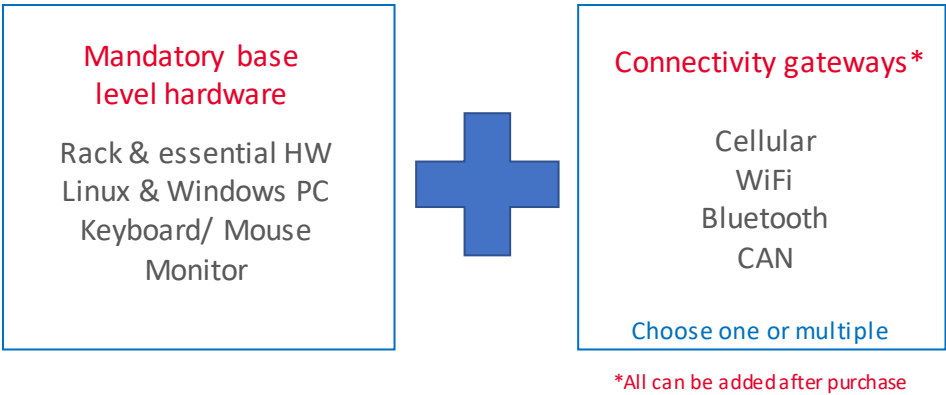


Figure 2. Steps for hardware configuration

Step 1. Mandatory Base-Level Hardware

Option Number	Option Description	Requirements
SA8710A-101	1x Microsoft Windows PC 1x Debian Linux PC 1x Keyboard 1x Mouse	Required at time of purchase
SA8710A-102	Monitor for system	Required at time of purchase

Step 2. Hardware to Connect to Your Device Under Test (DUT)

Choose at least ONE of the options below. All options can be retrofitted after the initial purchase. Part numbers for the upgrades are also shown.

Option Number	Option Description	Requirements
SA8710A-220	UXM 5G Cellular B Connectivity	4G/5G Can be retrofit
SA8710A-230	UXM 5G Cellular E Connectivity	4G/5G Can be retrofit
SA8710A-222	MXG N5182B with 503,656,660	Recommended for C-V2X interface
SA8710A-223	EXG N5172B with 503,653,660	Recommended for C-V2X interface
SA8710A-202	Hardware for Bluetooth connectivity	983-1107
SA8710A-212	Hardware for Bluetooth Fuzzing	983-1107
SA8710A-203	Hardware for WLAN connectivity	983-1106
SA8710A-213	Hardware for WLAN Fuzzing	983-1106
SA8710A-204	Hardware for CAN connectivity	983-1008
SA8710A-214	CAN HW +Vehicle Spy 3	983-1008
SA8710A-205	Hardware for Automotive Ethernet	Can be retrofit
SA8710A-215	Automotive Ethernet HW +Vehicle Spy 3	Can be retrofit

Upgrade Part Number	Option Description	Requirements
SA8711A-101	Cellular connectivity upgrade	For after initial purchase
SA8711A-102	Bluetooth connectivity upgrade	For after initial purchase
SA8711A-103	WLAN connectivity upgrade	For after initial purchase
SA8711A-104	CAN connectivity upgrade	For after initial purchase
SA8711A-105	Automotive Ethernet Connectivity Upgrade	For after initial purchase
SA8711A-114	CAN connectivity + Vehicle Spy 3 Enterprise upgrade	For after initial purchase
SA8711A-115	Automotive Ethernet connectivity + Vehicle Spy 3 Enterprise upgrade	For after initial purchase

After these two easy steps, you will have configured the hardware portion of the SA8710A solution. Next, software.

Software Configuration

Step 1. Mandatory Base Level and Pathwave Test* Software

Option Number	Option Description	Requirements
KS8400B	KS8400B PathWave Test	Required at time of purchase
SA8750B	IoT Security Assessment Automation Plugin	Require 983-1104 Base Controller

Step 2. Select the Additional Software

From the options below, Additional options can be added later, if required.

Option Number	Option Description	Requirements
SA8756B	CAN Fuzzing Software (Incl Cycur Fuzz)	SA8710A-204
SA8757B	V2X Fuzzing Test Plugin	Cellular HW(220 or 230), and C-V2X GNSS HW(222 or 223)
EP1501A	Pathwave Lab Ops for Automotive Cybersecurity	Can be retrofit
EP1510A	Base Vehicle Test	Can be retrofit
N7609EMBC	Signal Studio for Global Navigation Satellite System (GNSS)	Required for C-V2X Connectivity

Step 2.1 Choose the Cellular Connectivity Software

From the below options, if you choose SA8710A-220 or SA8710A-230 then please select below 4G/5G signaling option with IP Data option. Additional options (2G/3G/C-V2X) can be added later, if required.

Option Number	Option Description	Requirements
C8700200A	Test Application Framework	Cellular HW Required
C8730115A	LTE Rel-15 - Core Signaling	4G capability Cellular HW Required
C8735115A	5G NR Rel 15 - Core signaling	5G capability Cellular HW Required
C87300P1A	LTE IP Data	Require C8730115A
C87350P1A	5G NR IP Data	Require C8735114A
C8731108A	GSM Rel-8 signaling	2G capability Cellular HW Required
C8733113A	W-CDMA Rel-13 signaling	3G capability Cellular HW Required
C8732114A	C-V2X Rel14 PC5 signaling	C-V2X capability Cellular HW Required
CA8700B	ITS Functional Test Application	C-V2X capability Cellular HW Required
AV2030CNA	WaveBeeSting V2X fuzzing framework (China)	C-V2X capability Cellular HW Required

Step 3. Choose the Right IoT Security Assessment Software

From the below options, you must choose at least ONE that matches your hardware configuration. Additional options can be added later, if required.

Option Number	Option Description	Requirements
983-1104	Base Controller	IoT Security - Base Controller (Software, 1-year subscription)
983-1105	IPv4 Attack Module	IPv4 Attack Module + Application & Threat Intelligence Updates (Software, 1- year subscription)
983-1109	IPv6 Attack Module	IPv6 Attack Module + Application & Threat Intelligence Updates (Software, 1- year subscription)
983-1106	WLAN Attack Module	WLAN Attack Module + Application & Threat Intelligence Updates - (Software, 1- year subscription)
983-1107	Bluetooth Attack Module	Bluetooth Attack Module + Application & Threat Intelligence Updates - (Software, 1-year subscription)
983-1108	CAN-BUS Attack Module	CAN-BUS Attack Module + Application & Threat Intelligence Updates - (Software, 1-year subscription)
983-1110	IoT Security Bundle	(WLAN, Bluetooth, IP) + Application & Threat Intelligence Updates - (Software, 1-year subscription)

All the software options are 12-month subscription models; multi-year licensing is also available. You will need a valid subscription to be able to use the software, and to receive updates to the Keysight IoT Security Assessment. The Keysight IoT Security Assessment is consistently receiving updates for the latest threats detected by our research centers, so they best way to stay on top of cybersecurity is to ensure you are testing against the latest threats out there.

The IoT Security Bundle comes with Bluetooth, WLAN and IPv4 with Base Controller, customers will need to add the IPv6 module separately.

On top of the hardware and software, you can also rely on our Keysight world class team of experts for help and advice, both when specifying your system and after deployment.

Benefit from Flexibility

The key feature of the Keysight SA8710A is the flexibility the system allows:

- Buy what you need, when you need it.
 - If you are only interested in a cellular connection at the time of purchase, then only buy the hardware and software for cellular.
 - All the connectivity hardware and software can be added later.
- Keysight is continually working to add new connectivity options both for existing connection options and for new technologies as they arise.
- The Keysight subscription model allows you to spread the cost of development.
- With an active subscription, the Keysight IoT Security Assessment will receive constant updates to ensure you are able to stay a step ahead of emerging threats.
- Keysight will also strive to be a part of any emerging automotive cybersecurity standards organizations and bodies to ensure all tests made with our solution are traceable and conform to the highest standards.

Bluetooth® and the Bluetooth logos are registered trademarks owned by Bluetooth SIG, Inc., and any use of such marks by Keysight Technologies is under license.

cdma2000 is a US registered certification mark of the Telecommunications Industry Association.

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.



This information is subject to change without notice. © Keysight Technologies, 2020 – 2026, Published in USA, August 4, 2026, 3120-1411.EN