Instrument and Communications Security Overview

Instrument Function

Sofia 2[1] is a small bench top analyzer that uses advanced fluorescence detection with an ultraviolet LED energy source. Sofia 2 collects hundreds of data points on the test strip contained inside of a Sofia FIA Test Cassette. Sofia 2 uses proprietary algorithms to analyze the data, interpret the signals and determine the results automatically to give you an objective result you can rely on.

Sofia 2 offers an easy-to-use interface, customizable settings, flexible workflow, barcode technology and Virena® connectivity. Results are reported automatically on the screen and can be stored in Sofia 2, optionally printed on an external printer, sent to Virena or forwarded to other systems via standard data interfaces.[2]

Instrument OS

- Sofia 2 has a hardened Yocto Project® Linux® kernel with no operating system overlay.
- The Linux kernel would require complete recompilation to be compromised.
- It is purpose-built to support only the analyzer functions.

Instrument Kernel Security

- Sofia Administrator controls I/O and operational functions.
- Only the Sofia operational menus are accessible to Users.
- There is no capability to insert any foreign software.
- Root Kernel access is limited to Quidel Engineers via secure shell and each unit has its own unique large and complex key that is never shared.
- There is no "Remote Control" functionality.

Data at Rest

- Test result data stored unencrypted in eMMC flash storage.
- Data storage is fixed and cannot be removed.
- The Sofia Administrator may delete stored Patient Tests.

Instrument I/O

- Wi-Fi and Wired Ethernet Interfaces are available for instrument communications.
- LTE Wireless Interface is present for instrument communication to Virena.
- USB interface is available for USB printer interface and USB data import/export.
- Barcode scanner.

[1] https://www.quidel.com/immunoassays/sofia-tests-kits/sofia-2-analyzer
[2] https://connectme.quidel.com/docs/lis/sofia-2/

LAN Interfaces

- Wi-Fi supports secure communications via WPA2 with Pre-shared Key Protocol.
- Wired Ethernet is 10/100.

LTE Interface

Sofia 2 has a 4G LTE Radio to support communication of HIIPA compliant, de-identified test results to the Quidel Virena[3] cloud application over the Verizon Network. Virena is optional system support software.

USB Interface

- Sofia 2 has two USB ports. Supported use of the USB ports is for:
  - Printing results to an external USB Printer
  - Import/Export of User Lists and System Settings
  - Import of new System Firmware
  - Import of Assay Method Files
  - Import of Language Files
  - Export of System Log Files
  - Export of Test Results (if configured by Admin to support this)
- Access to USB configuration and Import/Export functionality is limited to the Sofia 2 Administrator via their password protected login.

Barcode Scanner Interface

The instrument has a built-in barcode scanner for reading 1 and 2d barcode types. The barcode scanner may be used to input data into the Operator ID, Patient ID and Order Number fields of Sofia 2. The scanner is also utilized to input the "QC Card" data when running External QC Controls.

LIS Interface

- Sofia 2 supports two industry standard interfaces for sending data to Laboratory Information Systems (LIS) or host systems that support LIS communication protocols. The support interfaces are:
  - ASTM (now officially CLSI LIS01-A2 and LIS2-A2)
  - POCT1a
- All LIS interface communication is over Ethernet or Wi-Fi.
- These industry standard interfaces support transmission of Sofia 2 test and QC results to upstream systems that support these common protocols. ASTM is generally used for sending to LIS systems while the point-of-care protocol (POCT1a) is supported by point-of-care data management systems like RALS™ and Telcor QML®. ASTM supports unidirectional communication while the POCT1a protocol supports Sofia 2 device management for loading instrument operators and setting the local time in Sofia 2.

[3] https://beinformed.quidel.com/what-is-virena/

LIS interface Security

Both LIS interface protocols send data across local area networks in clear text. Typically, the instruments are operated on private enterprise networks, often on micro segmented VLAN networks protected at the network edges by enterprise firewalls. Best practice for communication with remote host systems outside the firewalls would be over a VPN.

Sofia 2 holds and sends a limited data set of information considered Protected Health Information (PHI). There are two data entry fields that can be utilized during testing that may hold PHI. These fields most often receive a Patient ID or an LIS Accession Number or both. No other PHI is stored in Sofia 2.

Automated Firmware Updates

Sofia 2 Administrator may choose to implement Automatic Updates functionality as of firmware version 1.12. This feature allows Sofia 2 to communicate over Ethernet or Wi-Fi to Quidel's update servers and fetch Sofia 2 firmware updates as they become available. The Sofia 2 Administrator may choose when to install updates or set the instrument to apply them automatically. Quidel has partnered with Microsoft to utilize their secure IOT solution. Data transferred between the systems uses HTTPS communications that incorporate a combination of TLS 1.2, RSA 2,048-bit key lengths, and PFS encryption and security protocols.

To enable Automated Firmware Updates, some networks will need to allow-list the following ports and protocols.

Port	Transport Protocol	Protocol	Description	Domain Name
53	TCP / UDP	DNS	Domain Name System Resolution	N/A
123	UDP	NTP	Time Services	0.pool.ntp.org 1.pool.ntp.org
443	TCP	HTTPS	Device Registration	global.azure-devices-provisioning.net
			IoT Endpoint	connectedcustomer-hub-prod.azure-devices.net
			Registration Failure Service	cc-failed-registration.quidel-apps.com
			Internet connection check, File Download Service	data-cc.quidel-apps.com
			Log File Uploads	ccprodinternal.blob.core.windows.net

Automated Firmware Updates are optional. Customers who want to download Firmware Updates to USB Thumb Drive and apply updates via the legacy manual process may continue to do so. Sofia 2 will not attempt Automated Updates communication unless this function is enabled by the Sofia 2 Administrator. Manual firmware updates are available via https://myquidel.com

Virena Cloud Communications

Virena data contains calibration information, de-identified PHI Test and QC results information. Users who enable Automated Firmware Updates and who participate in Virena, will automatically have Virena communication switched from 4G LTE cell communication to Ethernet or Wi-Fi and Internet communications. Connection is to Microsoft Azure Servers using the same security protocols as Automated Firmware Updates.

Sofia 2 units that have not enabled Automated Firmware Update functionality but participate in Virena, will continue to communicate with Virena over Verizon's 4G LTE cell network. Virena communication over Verizon 4G LTE is encrypted. For legacy 4G LTE communication, Verizon provides data forwarding services to deliver Sofia 2 results to Digi® Corporation.[4] Quidel is partnered with Digi Corporation for transport of Virena Sofia 2 test results. Received data is stored encrypted at rest for minutes until our Virena servers query for new results. When results are saved to the Virena database, they are deleted from the temporary Digi Corporation storage. All communications between Digi and Virena are encrypted using HTTPS communications that incorporate a combination of TLS, RSA 2,048-bit key lengths, and PFS encryption and security protocols.

MI2029900EN00 (11/22)

[4] https://www.digi.com/products/iot-software-services/digi-remote-manager