TECAN.

Operating Manual

Secure Operating Manual

for Spark and Spark Cyto

including firmware and software:

- SparkControl
- Result Analyzer (including plugins: Counting, Area, Multi-Color, 3D Imaging, Processing, Evaluation)

Document Part No. 30287754
2026-08
Document Version No. 1.0

30287754 00

WARNING: Carefully read and follow the instructions provided in this document before operating instrument and software.

Notice

Every effort has been made to avoid errors in text and diagrams; however, Tecan Austria GmbH assumes no responsibility for any errors, which may appear in this publication.

It is the policy of Tecan Austria GmbH to improve products as new techniques and components become available. Tecan Austria GmbH therefore reserves the right to change specifications at any time with appropriate validation, verification, and approvals.

We would appreciate any comments on this publication.

Manufacturer
Tecan Austria GmbH
Untersbergstr. 1A
A-5082 Grödig, Austria
T +43 62 46 89 330
E-mail: office.austria@tecan.com
www.tecan.com

Copyright Information

Trademarks

The following trademarks are either trademarks or registered trademarks of Tecan Group Ltd., Männedorf, Switzerland, in major countries:

- Cell Chip™
- Magellan™
- NanoQuant Plate™
- Result Analyzer™
- Spark®
- Spark® Cyto
- SparkControl™
- Spark-Stack™
- Te-Cool™
- Tecan®
- TECAN – Logo®

For registered trademarks of third parties, see: https://www.tecan.com/intellectual_property/trademarks

Table of Contents

1 About this Manual

1.1 Scope of this Manual

This manual provides cybersecurity information for professional users and administrators of the multimode microplate reader instruments Spark and Spark Cyto, as well as the SparkControl reader control software (including the Counting, Area, Multi-Color, 3D Imaging, Processing and Evaluation plugins), and the Result Analyzer data analysis software.

This Secure Operating Manual applies to SparkControl software V5.0, Result Analyzer software V1.0, and the respective firmware of the Spark and Spark Cyto reader family (FW package V13.0), as well as all subsequent versions until a new edition of this manual is released.

For all released versions of this Secure Operating Manual, visit: https://www.tecan.com/knowledge-portal

For more information about the products listed above, refer to the corresponding Instructions for Use (IFUs) provided with each product.

1.2 Definitions, Acronyms and Abbreviations

Abbreviations / Terms	Description
ASM	Application Software Manual
CAN	Controller Area Network
FAS	Field Application Scientist
FSE	Field Service Engineer
FW	Firmware
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
IAM	Identity Access Management
IFU	Instructions for Use
IoT	Internet of Things
LTSC	Long-Term Servicing Channel (Microsoft)
Maintained Software	Software components for which Tecan notifies customers of known security risks and provides updates.
MFA	Multi-Factor Authentication
MQTT	Message Queuing Telemetry Transport
OS	Operating System
SBOM	Software Bill Of Materials
Supported Software	Third-party software components for which Tecan notifies customers of known security risks and the availability of compatible updates.
SW	Software
UMS	User Management System
VDR	Vulnerability Disclosure Report

2 General Information

Description	Information
Product Name	Spark, Spark Cyto
Software System Name	SparkControl, Result Analyzer
Software Application Name	SparkControl, Result Analyzer
Plugins	Counting, Area, Multi-Color, 3D Imaging, Processing, Evaluation
SBOM	Provided by Tecan upon request
Recommended Operating System	See IFU SparkControl

2.1 Supported Software

Tecan will monitor the availability of recommended security updates for supported third-party software used with this system.

For information on the compatibility of third-party software components and versions, refer to the applicable Software Release Notes on the provided USB drive.

During the preventive maintenance visit, the Tecan Service Engineer will inform the customer of recommended software updates for their system.

The following software items are classified as supported software:

- SAP Crystal Reports
- Microsoft .NET Framework
- Microsoft Visual C++
- Microsoft Visual C++ Redistributable

For a complete overview of the software components and versions, refer to the SBOM.
The SBOM is available upon request from the Tecan Helpdesk.

Customers are responsible for regularly checking the websites of other third-party software suppliers, including those for operating systems and antivirus software, for recommended security updates. Customers are also responsible for deciding whether to download and apply these updates to their systems.

Back up data files before starting any updates.

Perform Installation Qualification (IQ), Operation Qualification (OQ), and Performance Qualification (PQ) of software after every system modification.

2.2 Maintained Software

Tecan will initiate software and security updates for maintained software as needed.

Customers should regularly check the Software Release Notes on the Tecan Knowledge Portal for information on software and security updates:
https://www.tecan.com/knowledge-portal

Updates that enhance application software functionality are made available for ordering as software upgrades and can typically be installed by a professional user.

Firmware updates for the Spark and Spark Cyto instruments are available for installation by a Tecan Field Service Engineer (FSE).

Tecan recommends always using the latest available firmware package.

The following software items are classified as maintained software:

- **Tecan firmware packages** for Spark and Spark Cyto as embedded software on the instrument
- **Tecan software SparkControl** (incl. plugins) which is typically installed on the customer PC (in case of Spark Cyto: Spark Cyto control unit PC)
- **Tecan software Result Analyzer** which is typically installed on the customer PC (in case of Spark Cyto: the Spark Cyto control unit PC)
  Tecan software SparkControl Magellan which is typically installed on the customer PC (in case of Spark Cyto: the Spark Cyto control unit PC)

2.3 End of Life

At the time of publication of this Secure Operating Manual, no end-of-life date has been defined.

Tecan will typically announce product phase-out information two years in advance at:
https://www.tecan.com/phaseouts

Until end of life, technical security support is provided by Tecan.

3 System Overview

This chapter and the system diagram describe all external interfaces and applications connected to the system, providing an overview of its integration and dependencies.

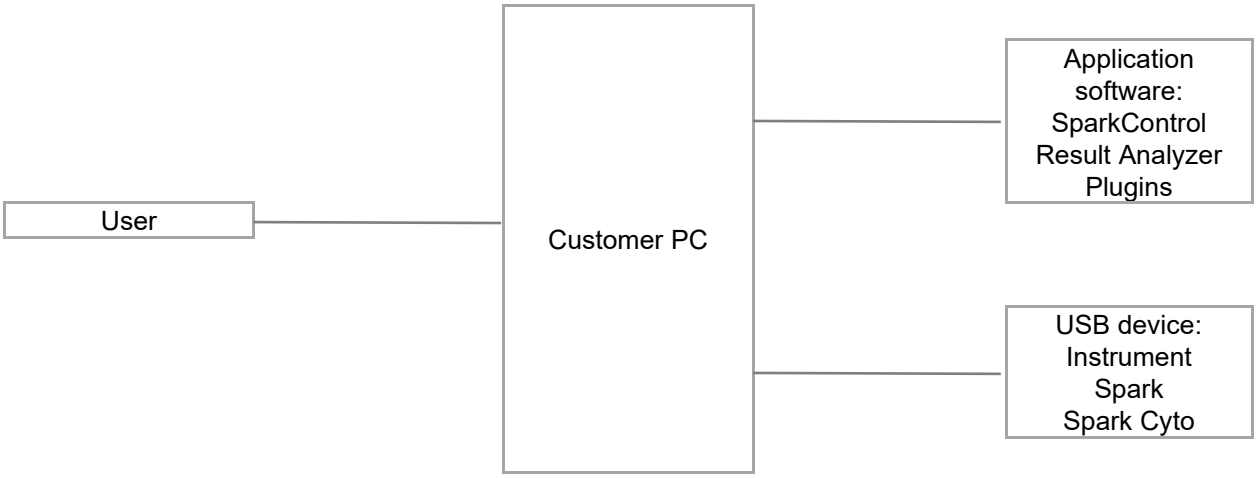

Fig.1: System diagram

The application software is used to control the reader and analyze data generated by measurements with the Spark or Spark Cyto multimode microplate reader, as described above.

The software does not generate, use, transmit, or store patient-related data. Instead, it only generates, uses, transmits and stores sample IDs and the corresponding results.

The software is designed to operate on a single computer and is not intended to be integrated into a network.

The system described above does not require internet access or access to a cloud-based system.

3.1 Description of External Interfaces

Name	Protocol	Purpose
User	-	PC login with Windows user password.
FSE	-	PC login with Windows user password (provided by customer).
Customer PC	USB	The customer PC is connected via a USB cable to the USB port of the instrument.
Spark Cyto Control Unit (Dedicated Spark Cyto PC)	USB	The Spark Cyto PC is connected via a USB cable to the USB port of the instrument.
Customer Screen	DP Mini-DP	The external screen is connected to the instrument PC.
Camera (Cell Module)	USB	The Spark Cell Module camera is connected via a USB 3.0 cable to the USB port of the customer PC.
Camera (FIM Module)	USB	The Spark FIM Module camera is connected via a USB 3.0 cable to the USB port of the Spark Cyto Control Unit.
Injector Module	CAN	The Spark injector module is connected to the instrument via a CAN cable.
Te-Cool Module	CAN	The Te-Cool module is connected to the instrument via a CAN cable.
SparkControl API	COM	Option to control SparkControl from external applications.
Generic USB device	USB	Communication with external storage and modules like keyboard and mouse.

4 User Access and Authentication

This chapter describes the available user types and roles and what needs to be considered during operation.

Physical access controls shall be in place as defined by local laboratory and facility regulations or GLP / GMP.

The customer's system administrator is responsible for any changes made to the operating system of the customer computer. The system administrator typically belongs to the customer's IT department and has full Windows administrator rights.

The system administrator or software administrator shall create personalized Windows user accounts for all device operators.

NOTE: For safe and secure operation, operators and key operators must not be granted Windows administrator rights. Tecan FSEs and FASs only require Windows administrator rights when installing, uninstalling or upgrading the software. Windows administrator rights should only be granted temporarily. Alternatively, these tasks can be performed by the customer's Windows administrator with guidance from a Tecan FSE or FAS.

A summary of the different roles and privileges is provided in the table below:

No.	User Group	User Subgroup	Windows Account and Privileges	Software Account and Privileges	Service SW Access
1	Software administrator (customer)	Administrator	"User" Read & execute	Full software admin rights	No
2	Application specialist (customer)	Professional user, Key operator	"User" Read & execute	Create and edit methods, no editing of signed methods	No
3	End user / Routine user (customer)	Operator	"User" Read & execute	"User" Execution of defined methods. Perform measurement and save results	No
4	System administrator (belonging to the IT department of the customer)	OS Administrator	"Admin" Full Windows admin rights	Optional	No
5	Tecan personnel	FSE, FAS	No Service SW is installed on the customer computer. Windows access rights to be provided by customer OS admin to Tecan personnel	No Windows access rights to be provided by customer admin to Tecan personnel in case of maintenance.	Service SW is used on the laptop of the Tecan FSE.

5 System Setup and Configuration

Please note that all displayed folder paths correspond to a US English Microsoft operating system.

5.1 Network Configuration

The software is designed to operate on a single computer and is not intended to be integrated into a network.

5.2 Anti-malware Software

Tecan recommends avoiding active scanning of hard drives or memory with anti-malware software while a measurement is in progress with the software.

If a virus scan must be performed during a run, exclude (whitelist) the following directories and their subdirectories from the scan:

- C:\Program Files (x86)\Tecan
- C:\Program Files\Tecan

5.3 Decommissioning of the System

Proper decommissioning of the system is the responsibility of the professional user.

Before deleting these folders, create a backup of your data:

- C:\Users\Public\Documents\Tecan

Tecan recommends the following actions when decommissioning the complete system:

- Activate the Window uninstall routine as described in the chapter “Uninstall/Repair Installation” in the IFU SparkControl.
- To securely remove user data, manually delete files in this folder:
  C:\Users\Public\Documents\Tecan

6 System Operation and Maintenance

Please refer to the following checklist during system operation and maintenance:

- Customers should regularly review the Software Release Notes on the Tecan Knowledge Portal for information about software and security updates:
  https://www.tecan.com/knowledge-portal/

- Back up data files before starting any updates or making changes to the system.

- Customers should perform regular backups of their system to ensure that they can recover their data in the event of incidents, such as cyberattacks.

  For more information, please refer to the Chapter “System Requirements” in the IFU SparkControl or the Chapters “Cybersecurity Information” and “Archive Files” in the IFU SparkControl Magellan.

- Users shall always shut down the system and the running software properly.

- Disconnecting the power cable while the system is operating, or closing the application software by shutting down the operating system may cause the system to enter a state similar to a power outage.

- Tecan recommends shutting down and restarting the system periodically to avoid performance problems.

- In addition to the installation qualification check, Tecan also recommends that the calculation abilities of SparkControl Magellan are tested. For a detailed description, refer to chapter “Cybersecurity Information” in the IFU SparkControl Magellan.

7 Security Controls

The following security risks cannot be fully mitigated by the system described in this manual. Therefore, customers should implement the following security controls to reduce the risk of cyberattacks:

Risk	Mitigation
An attacker could attempt to gain physical access to the laboratory where the system, comprising the customer PC running the software and the multimode microplate reader, is located. The objective of such an attack is to compromise data files and make the system inoperable. Attackers can directly interact with the hardware, allowing them to tamper with the system, access data, or bypass security mechanisms. Attackers can modify hardware or access physical ports (e.g., USB), access or steal hard drives containing data and information, or even destroy the hardware.	• A physical access control shall be in place as defined by local laboratory and facility regulations, or GLP / GMP. • Set up Windows access control and ensure system operators have the lowest suitable access rights. • Regular backup of data files in a secure location • For SparkControl Magellan: Utilize the archive feature in the SparkControl Magellan software to regularly back up data files. • For SparkControl Magellan: Use the Tracker version of the Magellan software, which supports 21 CFR part 11 functionality, to control access and enhance application security.
An attacker could attempt to gain system access by systematically trying multiple passwords.	• Implement a password policy that includes password strength requirements, complexity rules, password update rules, and rules prohibiting password sharing across different systems. • Enable email notifications to the software administrator when an account is locked due to multiple failed password attempts.
Reusing a password from another system can allow an attacker to gain access to the system if the password is compromised.	• Implement a password policy that includes password strength requirements, complexity rules, password update rules, and rules prohibiting password sharing across different systems. • Enable email notifications to the software administrator when an account is locked due to multiple failed password attempts.
Attack via an open internet connection.	• The system operates independently of internet or cloud access. Therefore, the customer PC should remain disconnected from the internet.
An attacker could attempt to target data files exported from the software to a Laboratory Information Management System (LIMS).	• It is the responsibility of the operating authority to protect data on the LIMS server against attacks.
Unauthorized data modification or falsification	• To prevent the misuse of user rights and falsification of data, it is recommended that the Windows user management administrator does not have software user rights. Ideally, the Windows user management administrator should belong to the IT department (system administrator). • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level.

Risk	Mitigation
Database (Master and workspace): External manipulation of data Database can be modified, manipulated or deleted through unauthorized access.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location • Lost data (incl. settings, methods) can be recovered/imported from previous backups.
An attacker gains access to Windows Communication Foundation (WCF) services, leading to unauthorized access, data tampering, or impersonation attacks.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location
An attacker gains access to gRPC (Remote Procedure Call) services, leading to unauthorized access to data and data manipulation.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location
An attacker can manipulate, corrupt or delete the G-factor calibration configuration files. Files can be changed undetectably.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location
Log files can be deleted, modified or corrupted without detection. An attacker can delete or alter logs to hide traces of malicious activities.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location
Corrupted, wrong or missing data due to undiscovered security incidents. Missing logging and monitoring mechanisms in case of a cybersecurity attack.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location

Risk	Mitigation
All application data (workspaces) is stored in a local, public directory to which all logged-in users have full access. This means that logged-in users could read, manipulate or even delete data.	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location
An attacker injects malicious XML content into an application's XML input or query (method definition XML files). This can manipulate the logic of XML parsers or execute unauthorized actions, such as data extraction, data corruption, data loss, bypassing access controls, or cause denial of service (DoS).	• Set up Windows access control and ensure system operators have only the minimum access rights required for their tasks. • The software is designed to be operational with standard Microsoft user rights. Ensure that users are granted only the minimum level of privileges required at the Microsoft Operating System level. • Regular backup of data files in a secure location

7.1 Open vulnerabilities

For information on open vulnerabilities and their corresponding risk control measures, please refer to the Software Release Notes.

If you require a Vulnerability Disclosure Report or want to report any discovered vulnerabilities, please contact the Tecan Helpdesk.

For contact information, visit: https://www.tecan.com/support

7.2 Contact in case of a security incident

In the event of a cybersecurity incident involving these products, please report the incident to the Tecan Helpdesk.

For contact information, visit: https://www.tecan.com/support

Tecan Customer Support

If you have any questions or need technical support for your Tecan product, please contact your local Tecan Customer Support team.

For contact information, visit: https://www.tecan.com/support

Before contacting Tecan for product support, please have the following information ready for optimal technical assistance (refer to the instrument's name plate):

- Model name of your product
- Serial number (SN) of your product
- Software and software version (if applicable)
- Description of the problem and contact person
- Date and time when the problem occurred
- Steps that you have already taken to correct the problem
- Your contact information, including phone number and e-mail address